High Level Design netwerk en beveiliging ROC FP v1.1

Functioneel Ontwerp

Datum	21-03-2022
Auteur(s)	Design Office ROC FP
Versie	1.1
Status	Definitief

Inhoudsopgave

Documentbeheer

Revisiegeschiedenis

Versie	Opmerkingen
0.1	Opzet document
0.2	Verdere invulling HLD
0.3	Afronding invulling HLD
1.0	Vaststelling door gremium Design Office ROC FP
1.1	Minimale update o.b.v. peer review Design Office ROC FP

Distributielijst

Marktpartijen aanbesteding.

Contactpersonenlijst

Zie aanbestedingsdocumentatie.

Relatie met andere documenten/brondocumentatie

Document/bronbestand	Status	Auteur
Techniek Architectuurblauwdruk domein security v1.0	Definitief	Design Office ROC FP
Techniek Architectuurblauwdruk domein netwerk v1.0	Definitief	Design Office ROC FP

Classificatie

	Categorie	Toelichting
	Laag	Informatie geschikt voor algemene publicatie en externe distributie.
✓	Midden	Informatie die gevoelig is en enkel bestemd voor een beperkte groep.
	Hoog	Informatie die zeer gevoelig is en enkel bestemd voor specifiek benoemde personen.

1 Inleiding

1.1 Achtergrond

Dit document bevat het High Level Design (HLD) voor het netwerk en de beveiliging hiervan van ROC FP. Het document moet worden gelezen in samenhang met de blauwdrukken voor het netwerk en de security hiervan en met het document 'ROC FP Poortbezettingen, dimensionering en SLA'.

1.2 Indeling van het document (leeswijzer)

Het document is als volgt ingedeeld:

- **Hoofdstuk 1: Introductie**
  Dit hoofdstuk bevat een korte introductie van het document.

- **Hoofdstuk 2: Contextueel niveau (Waarom?)**
  In dit hoofdstuk wordt de '*waarom-vraag'* ten aanzien van de oplossing beantwoord. Onderwerpen die de revue passeren zijn: de visie, doelstellingen, scope van het document, de stakeholders, beperkingen, risico's, uitgangspunten, afhankelijkheden et cetera.

- **Hoofdstuk 3: Conceptueel niveau (Wat?)**
  In dit hoofdstuk wordt de '*wat-vraag'* ten aanzien van de oplossing beantwoord. Wat wordt gerealiseerd met de beoogde oplossing? Wat zijn de bestandsdelen (bouwblokken) die direct of indirect te maken hebben met de beoogde oplossing?

- **Hoofdstuk 4: Logisch niveau (Hoe?)**
  In dit hoofdstuk wordt de beoogde oplossing vanuit een functioneel perspectief beschreven, waarbij gebruikgemaakt wordt van de bouwblokken waaruit de oplossing is opgebouwd. De logische componenten van de oplossing worden hierbij beschreven en geïllustreerd.

- **Appendix A: Gebruikte afkortingen**
  In dit onderdeel zijn alle in dit HLD gebruikte afkortingen uitgeschreven.

- **Appendix B: Uitwerking ontwerpregels architectuurblauwdruk architectuurgebied netwerk**
  Dit is een separate deliverable waarin de onderbouwing van betreffende ontwerpregels op het gebied van het netwerk is opgenomen. Waar nodig wordt verwezen naar dit HLD.

- **Appendix C: Uitwerking ontwerpregels architectuurblauwdruk architectuurgebied security**
  Dit is een separate deliverable waarin de onderbouwing van betreffende ontwerpregels op het gebied van security is opgenomen. Waar nodig wordt verwezen naar dit HLD.

1.3 Verklarende woordenlijst

Nr.	Document
Uxx	Uitgangspunt
Rxx	Risico
Bxx	Beperking
BPxx	Best Practice
DAxx	Dienstafhankelijkheden
PAxx	Projectafhankelijkheden
CBxx	Cloud Bouwblok
NBxx	Non-Cloud Bouwblok
SBxx	Security Bouwblok
OKxx	Ontwerpkeuze
Uxx	Uitgangspunt

Functionaliteiten in dit High Level Design zijn generiek beschreven. Eventuele terminologie die (mogelijk vaker) gebezigd wordt door een bepaalde vendor of eventueel aan een bepaalde vendor kan worden toegeschreven, is louter gebaseerd op toeval. Het ROC FP is van mening, dat gevraagde functionaliteiten in dit HLD door verschillende vendors technisch kunnen worden ingevuld.

2 Contextueel niveau (Waarom?)

2.1 Visie

Het ROC Friese Poort (in het vervolg ROC FP) wil een aanbesteding uitschrijven voor een modern, toekomstbestendig, flexibel en veilig netwerk. Na de uiteindelijke gunning dient dit netwerk flexibel te kunnen meebewegen met de functionele vragen vanuit het 'werkveld' van ROC FP. Er moet bijvoorbeeld flexibel kunnen worden opgeschaald en afgeschaald in omvang van de installed base, de aantal WAN-/internetverbindingen en de bandbreedte van deze WAN-/internetverbindingen. Het ROC FP is hierbij op zoek naar een partner die maximaal met ons meedenkt, ons van advies voorziet en trends/ ontwikkelingen voor ons kan duiden die betrekking hebben op ons werkveld. Met andere woorden: ROC FP is op zoek naar een strategische partner die ons maximaal ontzorgt.

2.2 Doelstellingen HLD

De doelstelling van het HLD is het beschrijven van alle netwerk- en securitygerelateerde functies die het ROC FP voor ogen heeft. Hoe de functionaliteiten daadwerkelijk technisch worden ingevuld, wordt aan de winnaar van de aanbesteding overgelaten. Het HLD in combinatie met de bijlagen waarin de ontwerpregels zijn 'onderbouwd' bieden onzes inziens voldoende handvatten om het functioneel uitgevraagde als dienst (NAAS: Network As A Service, incluis navenante securityfuncties) te kunnen aanbieden.

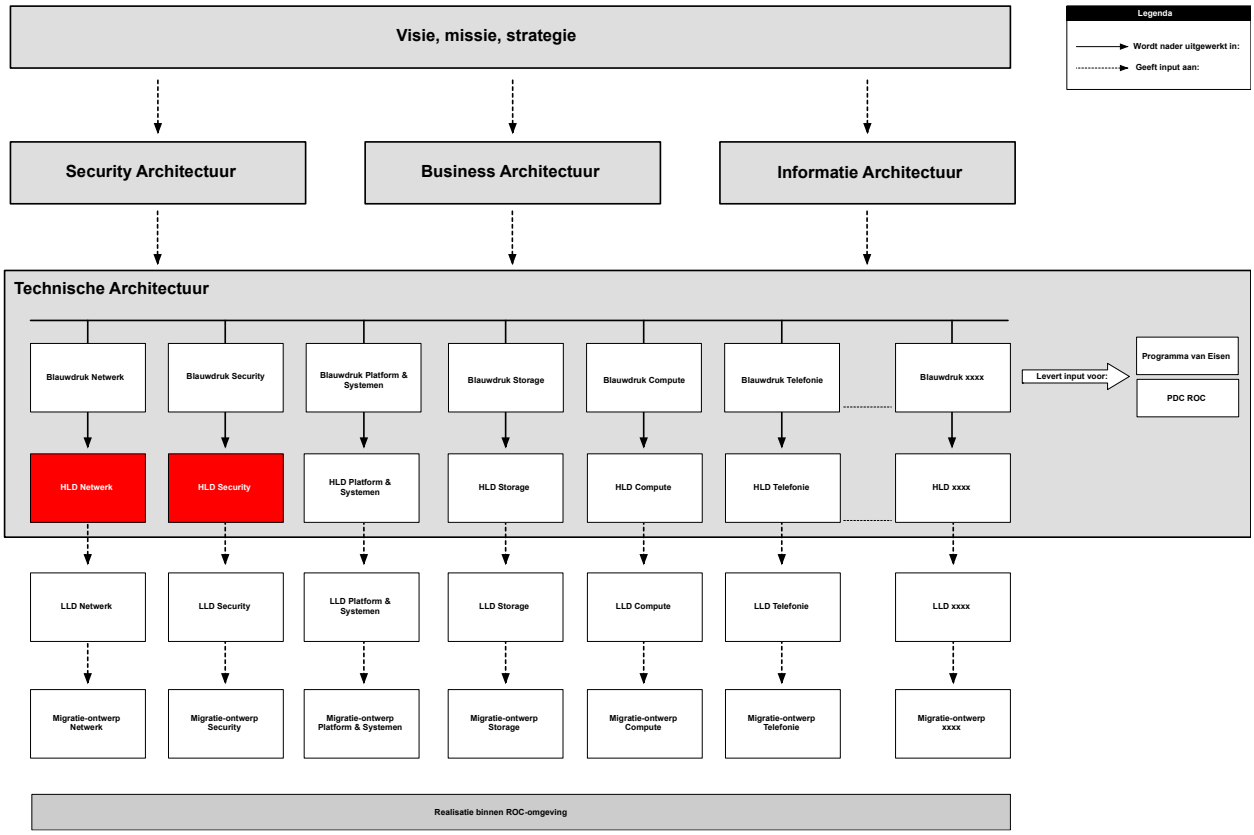
2.3 In scope

De scope van dit HLD betreft:

- LAN- en securitygerelateerde functies op locaties,
- WLAN- en securitygerelateerde functies op locaties,
- DC-LAN- en securitygerelateerde functies in de on-premises datacenters,
- Centrale on-premises firewall in de datacenters,
- WAN (en securitygerelateerde functies) tussen alle locaties en de on-premises datacenters,
- De internetontsluitingen,
- NAC (e.g. IEEE 802.1x/MAB, posture assessment, profiling).

In de figuur op de volgende pagina is de positie van dit HLD afgebeeld binnen de kaders van de technische architectuur.

Let op: Azure-onderdelen vallen buiten de scope van de aanbesteding. Deze onderdelen zijn echter wel bewust verwerkt in dit HLD, zodat de inschrijver a). Weet dat Azure een rol kan gaan spelen in de (nabije) toekomst en b). De zienswijze van het ROC FP begrijpt waar het de netwerk- en security-gerelateerde aspecten van Azure betreft.



Figuur 2-1: *HLD als deliverable binnen de technische architectuur*

2.4 Stakeholders

Stakeholder	Betrokkenheid	Belang
Lead architect Design Office	Conformiteit met technische blauwdruk netwerk	Quality Assurance rol. De functionele uitwerking van onderdelen in dit HLD zijn gebaseerd op de technische architectuurblauwdruk architectuurdomein netwerk. Functies dienen derhalve in lijn te zijn met de ontwerpregels vanuit deze blauwdruk.
Lead architect Netwerk	Conformiteit met technische doelarchitectuur	De functionele uitwerking van netwerkonderdelen in dit HLD zijn gebaseerd op de technische architectuurblauwdruk architectuurdomein netwerk. Functies dienen derhalve in lijn te

		zijn met de ontwerpregels vanuit deze blauwdruk.
Manager Operationeel Beheer	Kwaliteit technische dienstverlening	Het daadwerkelijk conform SLA aanbieden van technische automatiseringsdiensten aan klanten van het ROC gebeurt door de operationele afdeling(en) van het ROC FP. Manager Operationeel Beheer is op dit vlak derhalve operationeel eindverantwoor-delijke.
Service Level Management	Volledigheid PDC/ dienstenportfolio	Het ROC FP heeft als missie om het primaire en secundaire proces maximaal te ondersteunen bij het halen van zijn doelstellingen. Deze ondersteuning bestaat uit automatiseringsdiensten die geleverd worden via (standaard) producten en services uit de PDC.
Security Architect	Conformiteit met security doelarchitectuur	De Security Architect verifieert of security-onderdelen in het HLD zijn samengesteld conform de beschrijvingen en ontwerpregels in de technische architectuur-blauwdruk architectuurdomein security.

2.5 Projectafhankelijkheden

Volgnr	Project	Afhankelijkheid
PA01	SER-MER	Locatiesubnetten worden uit de infrastructuur van de MER verwijderd.
PA02	IEEE 802.1x	IEEE 802.1x wordt op het bedrade netwerk aangebracht.
PA03	BYOD	Brede uitrol van BYOD in het onderwijs vereist het uitnutten van de baten van NaaS.
PA04	Fusie FP-Friesland College	De fusie heeft rechtstreeks invloed op de doorlooptijd van het contract.

2.6 Dienstafhankelijkheden

Volgnr	Dienst	Afhankelijkheid	Eigenaar/team
DA01	Azure Active Directory	Identity store voor IEEE 802.1x en hybrid joined machines	ICT backoffice ROC FP
DA02	Active Directory	Identity store voor IEEE 802.1x/MAB	ICT backoffice ROC FP
DA03	Intune	Identity store voor device compliancy	ICT backoffice ROC FP
DA04	DCI (Datacenter Interconnect)	Communicatienetwerk tussen de on-premises-datacenters voor onder meer clustering van nodes	KPN
DA05	SURF internet	Internetconnecties in de on-premises-datacenters voor SD-WAN en DIA (Direct Internet Access)	SURF/backoffice infra
DA06	Toegang Azure	RBAC voor beheer netwerkgerelateerde/security-gerelateerde onderdelen binnen Azure	ICT backoffice ROC FP

2.7 Eisen

Met referte aan betreffende eisen (ontwerpregels) in de documenten:

- Techniek Architectuurblauwdruk architectuurgebied Netwerk,
- Techniek Architectuurblauwdruk domein Security.

2.8 Beperkingen

Volgnr	Beperking
B01	Er zijn locaties waarbij de WAN-/internetontsluiting niet van ROC FP is.

2.9 Uitgangspunten

Volgnr	Uitgangspunten
U01	Leden projectteam ROC FP zijn voldoende materiedeskundig.

2.10 Risico's

Volgnr	Risico	Gevolg	Maatregel	Kans	Impact
R01	Invoering van PEP-functies op SD-WAN-niveau kunnen mogelijk het budget overstijgen.	Dit kan gevolgen hebben voor betreffende security-vereisten t.a.v. de DIA.	In overleg met de markt nagaan welke PEP-functies eventueel niet noodzakelijk zijn. In overleg met de markt vaststellen of bepaalde PEP-functies niet op SD-	M	M

			WAN-niveau maar in de centrale on-premises-firewall kunnen worden aangebracht, waarbij een deel van het verkeer via het centrale model wordt omgeleid naar het on-premises-datacenter om daar te worden ‘afgehandeld’.		

3 Conceptueel niveau (Wat?)

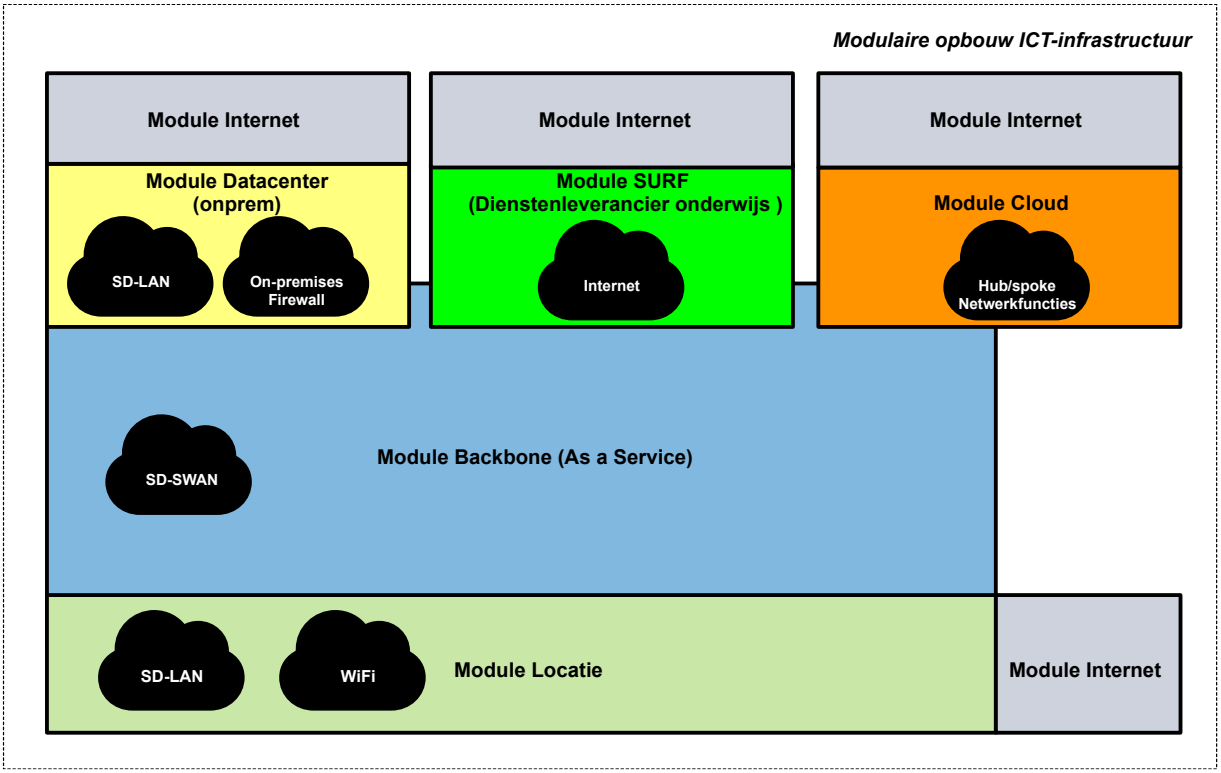
3.1 IST-situatie (de huidige situatie)

Voor de IST-situatie wordt verwezen naar het document ‘ROC FP Poortbezettingen, dimensionering en SLA’.

3.2 SOLL-situatie (de doelsituatie)

3.2.1 Modules technische infrastructuur

In de architectuurblauwdrukken van het ROC FP is de onderstaande modulaire opbouw van de ICT-infrastructuur opgenomen. In dit HLD wordt niet expliciet stilgestaan bij deze modulaire opbouw. De verschillende 'netwerkwolken' zijn de onderdelen/domeinen die in dit HLD worden beschreven.



Figuur 3-1: *Domeinen HLD gemapped op de modulaire opbouw van de ICT-infrastructuur*

Module	Domein HLD
Locatie	SD-LAN en WiFi
Backbone-as-a-Service	SD-WAN
On-premises-datacenter	Datacenter on-premises Anne Wadmanwei, Datacenter on-premises Wilaarderburen,
Module SURF	Internetconnectiviteit. Diensten die van SURF worden afgenomen verlopen via het internet. Middels deze internetconnectiviteit worden ook de volgende VPN-/IAAS-diensten ontsloten: • Konica Site-to-Site-VPN, • Cloud365 Horecaapplicatie in Sneek, • Eduarte databasesynchronisatie. • Remote beheer- en medewerkerstoegang • Pharmacom printing

Module internet	SD-WAN (met internet als onderliggende drager/transport)
Module Cloud	Azure, SaaS t.b.v. mgmt. en controlfuncties

3.2.2 Locatietypen

Het ROC beschikt over twee typen locaties, te weten:

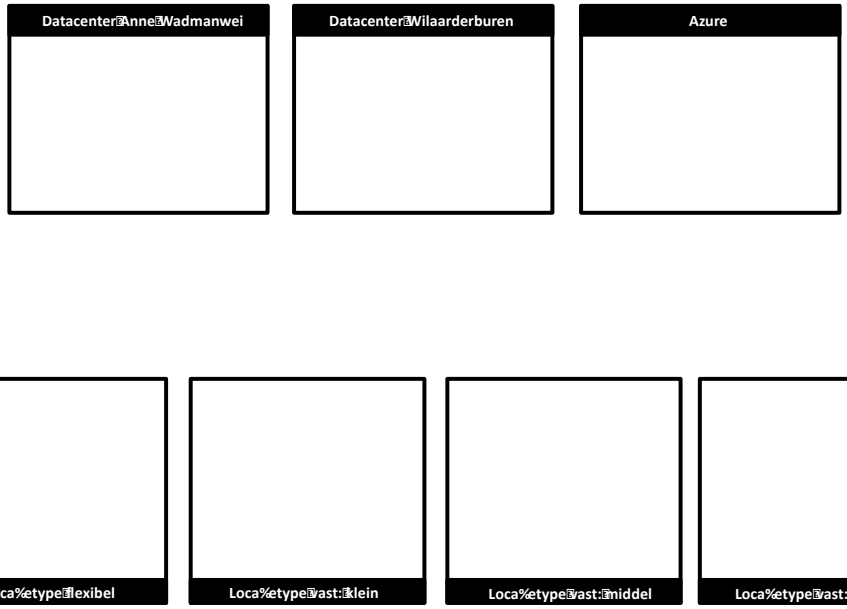
1. Vaste locaties,
2. Flexibele locaties.

Ad 1. Vaste locaties
Dit type locatie staat voor een permanente locatie van het ROC FP. Dit type locatie heeft geen korte levensduur en het ROC FP voert de volledige regie uit.

Ad 2. Flexibele locaties
Dit type locatie is tijdelijk van aard en kent derhalve een korte levensduur. Doorgaans is het ROC FP ook geen pandeigenaar en zodoende is het ROC FP dan ook afhankelijk van de door de pandeigenaar geboden dienstverlening (e.g. een (gedeelde) internetverbinding).

In dit HLD wordt verder geen onderscheid gemaakt in de geboden ICT-dienstverlening. Immers, op alle typen locaties dient in principe dezelfde dienstverlening te kunnen worden aangeboden waarbij de gebruikers van de services het netwerk als ‘standaard commodity’ beschouwen. Het netwerk c.q. de communicerende netwerkservices zijn voor gebruikers transparant. Let op: gebruiker in deze context kan ook een ICT-middel als een IoT-device of een printer zijn.

In de onderstaande illustratie zijn de locatietypen afgebeeld. Dit betreft naast de flexibele en vaste locaties ook de datacenterlocaties (on-premises) van het ROC FP en de clouddatacenterlocatie Azure.



Figuur 3-2: *Locatieoverzicht ROC FP (high level)*

De vaste locaties zijn onderverdeeld in drie categorieën:

1. Locatietype klein[1],
2. Locatietype middel,
3. Locatietype groot.

Deze categorisering is louter gebaseerd op de aantallen medewerkers, studenten en docenten per locatie van het ROC FP. Er dient echter wel rekening te worden gehouden met de faciliterende netwerkcomponenten om de dienstverlening op alle categorieën locaties optimaal te laten verlopen. In concrete komt het neer op de dimensionering en aantallen netwerkcomponenten per categorie.

De overige locaties zijn datacenterlocaties:

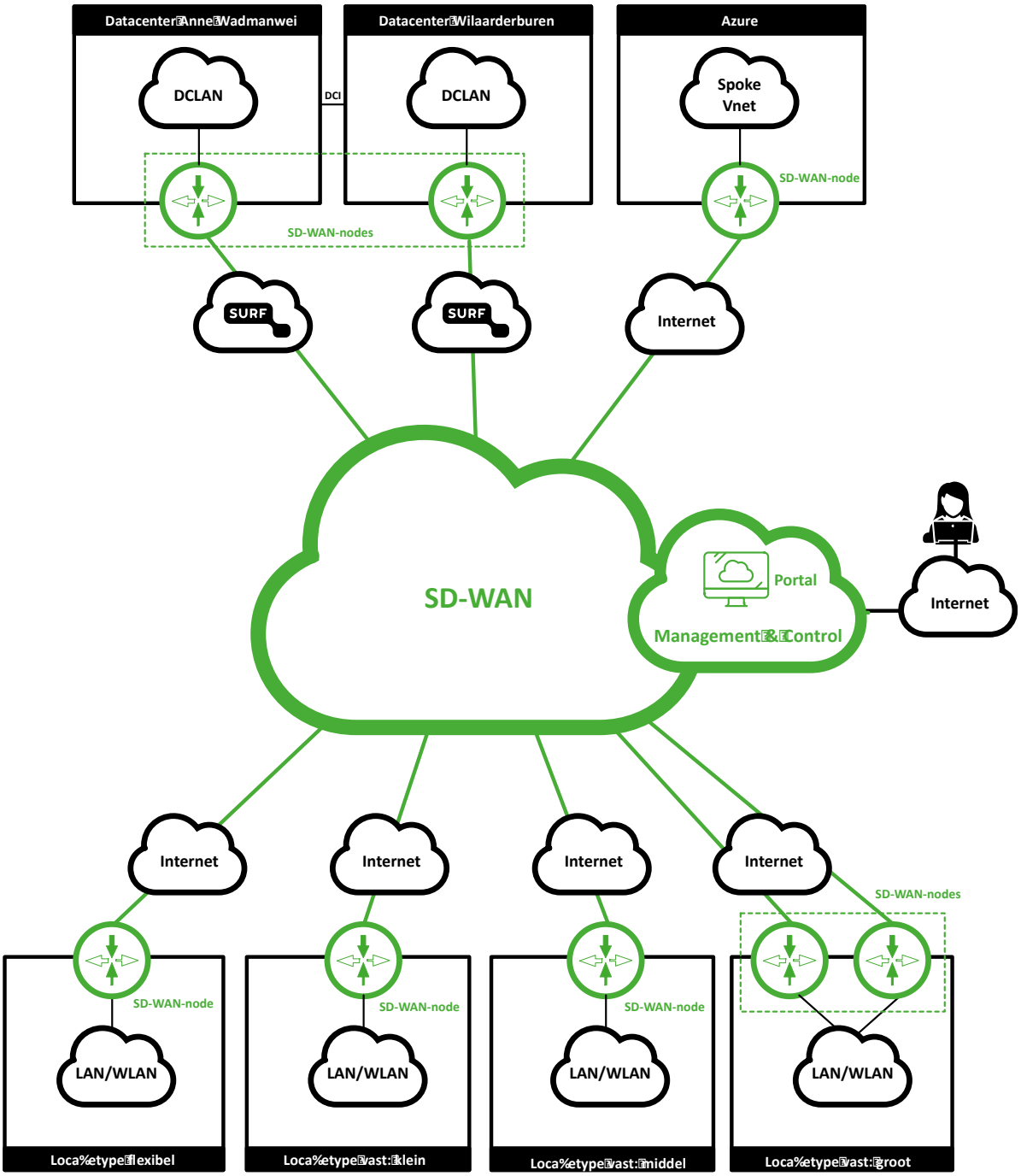
1. Datacenter on-premises Anne Wadmanwei,
2. Datacenter on-premises Wilaarderburen,
3. Clouddatacenter Azure.

In dit HLD zijn de functionaliteiten afgebeeld en beschreven die noodzakelijk zijn om de dienstverlening die het ROC FP aan zijn gebruikers biedt te kunnen accommoderen vanuit netwerktechnisch- en informatiebeveiligingsperspectief.

[1] Let op: ook locatietype flexibel behoort tot deze categorie.

3.2.3 SD-WAN

In de onderstaande illustratie is de WAN-connectiviteit tussen de typen locaties en datacenterlocaties (on-premises, Azure) high level afgebeeld. De WAN-technologie die deze connectiviteit mogelijk maakt, is gebaseerd op de principes van Software Defined WAN oftewel SD-WAN.



Figuur 3-3: *WAN-connectiviteit tussen locaties middels SD-WAN-technologie (high level)*

De IT-industrie verandert en evolueert voortdurend. Naarmate de tijd verstrijkt, is er een steeds grotere hoeveelheid technologieën die het WAN-netwerk onder druk zetten. Nieuwe paradigma's worden gevormd terwijl andere worden uitgefaseerd. Er worden nieuwe ontwikkelingen geconcipieerd en toegepast binnen de netwerkwereld. Vernieuwing van paradigma's leidt tot innovatie en de mogelijkheid om relevante technologieën op een vereenvoudigde manier toe te passen. Enkele vernieuwingen, trends en ontwikkelingen in dit kader zijn de volgende:

- Kunstmatige intelligentie (AI),
- Machine learning (ML),
- Clouddiensten
- Virtualisatie,
- Internet of Things (IoT).

3.2.3.1 Kenmerken van SD-WAN (i.e. functies die ondersteund worden)

Transportonafhankelijkheid/drageronafhankelijkheid

SD-WAN maakt gebruik van een transportonafhankelijke fabric-technologie die wordt ingezet om locaties van het ROC FP met elkaar te verbinden. Dit wordt bereikt door gebruik te maken van een overlay-technologie. De overlay tunnelt hierbij het verkeer over elk soort transportmedium tussen iedere bestemming binnen de SD-WAN-omgeving. In het geval van de locaties van het ROC FP worden internetcircuits gebruikt als transportmechanisme/drager (i.e. de underlay) van het overlay netwerk. Door over een fabric-overlay-netwerk te beschikken, is iedere locatie altijd een enkele hop verwijderd van een andere locatie.

Vereenvoudigd beheer

SD-WAN maakt de implementatie van WAN-services op locatieniveau snel en eenvoudig. Op grond van de 'cloud, tenzij strategie' van het ROC FP is de aansturing van het SD-WAN gebaseerd op een centrale cloudarchitectuur zoals is af te leiden uit figuur 3-3 (Management & Control functies). Op grond van deze strategie wordt uitgegaan van een controller als SaaS-dienst. Hiervan kan eventueel worden afgeweken, indien dit technologisch gezien een betere oplossing voortbrengt of waarbij het kostenaspect een andere oplossing dan een cloudoplossing rechtvaardigt. Kosten voor de oplossing (al dan niet als SaaS-dienst) behoren tot de NAAS-dienstverlening. De implementatie wordt op basis van zero-touch automatisch uitgevoerd middels één beheerinterface; implementatie- en configuratietijden worden hierbij verkort in tegenstelling tot traditionele WAN-oplossingen.

SLA/inzicht in applicaties, verkeersstromen

SD-WAN biedt de mogelijkheid om een SLA te bieden voor kritieke toepassingen/applicaties. Dit wordt bereikt door verkeer te kunnen routeren op basis van de ingegeven/vastgelegde applicatievereisten in de centrale beheeromgeving (zie figuur 3-3 | portalfunctie). Deze portal biedt ook statistieken over hoe de applicaties presteren, welke issues er zijn en welke trends zich voordoen. Op basis van de ingegeven policy bepaalt de SLA of de toepassing/applicatie zich aan die policy houdt en daarmee wel/niet goed

presteert of dat er enige issues zijn zoals jitter, verlies of vertraging van IP-pakketten. Als dit het geval is, kan de applicatie worden gerouteerd naar een ander transportmechanisme (mits voorhanden zoals bij het type grote locatie) dat ervoor zorgt, dat de applicatie aan de policy voldoet en daarmee aan de vastgelegde SLA. Door gebruik te maken van Artificial Intelligence/Machine Learning wordt real-time inzicht in de gehele infrastructuur verkregen. AI/ML wordt hierbij ook gebruikt voor trendanalyse m.b.t. capaciteitsvraagstukken (anticipatie), real-time inzicht in en het verhelpen van security-gerelateerde issues, inzicht in netwerk- en applicatieve verkeersstromen en issues in dat kader met real-time aanpassingen/ correcties. AI/ML doet dit alles aanzienlijk sneller en correcter op grond van datapatronen dan 'het menselijke oog en navenante interventie'. Tevens kan op gebruikersniveau worden ingezoomd. Issues in het netwerk worden centraal visueel zichtbaar gemaakt via de portal, waardoor efficiënt kan worden getroubleshoot. De cloudoplossing voorziet in ketenanalyse van een issue en stelt oplossingen voor op grond van best-practices.

Verhoging van behendigheid

Met SD-WAN is het mogelijk om eenvoudig WAN-verbindingen toe te voegen of te verwijderen en om mobiele en vaste verbindingen te combineren (indien noodzakelijk). Zo is het bijvoorbeeld mogelijk het type locatie flexibel te voorzien van een 4G/5G mobiele node die als drager (underlay) acteert binnen het SD-WAN-netwerk. Tevens is het mogelijk om de internetcircuit(s) van de pandeigenaar te gebruiken als drager (underlay), waarbij alsnog de locatie deel uitmaakt van de SD-WAN-fabric.

Zonering

Zonering is een andere use case/motivatie voor het gebruik van SD-WAN-technologie. Vaak hebben organisaties verschillende afdelingen die gescheiden moeten worden. Studenten moeten bijvoorbeeld worden gescheiden van IT-middelen als printers. SD-WAN-technologie voorziet hier eenvoudig in door gebruik te maken van VPN-verbindingen binnen het WAN. Zie voor meer informatie paragraaf 3.2.8.

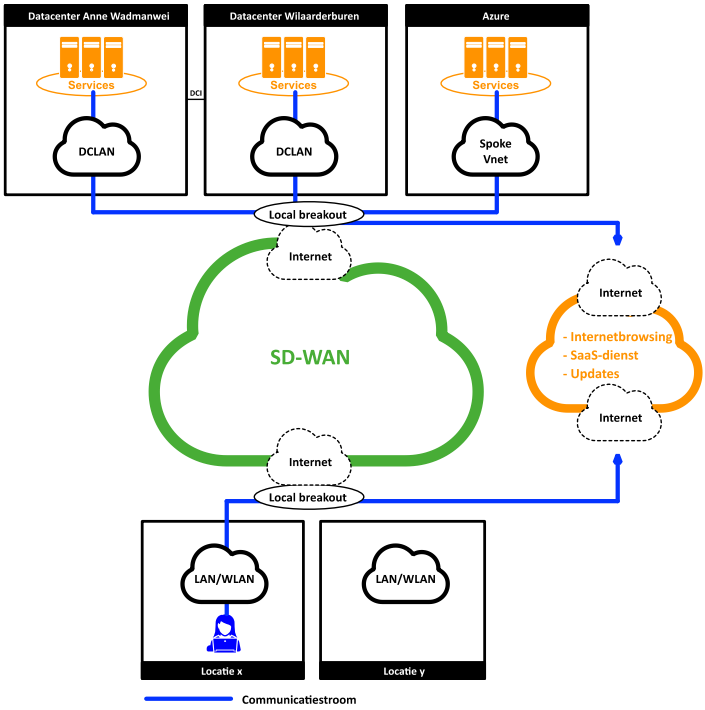
DIA (Direct Internet Access (DIA)

Eén van de meest in het oog springende use cases in het kader van SD-WAN-technologie betreft de mogelijkheid om lokaal het internet te benaderen vanaf ieder type locatie (dus geen gebruik maken van een centrale internetopgang die vanuit een on-premises-datacenter wordt geleverd in het traditionele internettoegangsmodel). De DIA-functie biedt zodoende de mogelijkheid om verkeer rechtstreeks de lokale internetopgang op te sturen in plaats van het helemaal terug te leiden naar een gecentraliseerd on-premises-datacenter (i.e. hairpinning). Hierdoor kunnen cloud-based- applicaties rechtstreeks het internet benaderen, zonder onnodig WAN-bandbreedte te gebruiken en hairpinning van verkeer in het on-premises-datacenter te veroorzaken.

Integratie SD-LAN/WiFi

Idealiter behoort integratie met het SD-LAN/WiFi tot de mogelijkheden, waarbij alle functies van SDN middels de centrale cloudomgeving samenkomen voor een optimaal end-to-end-inzicht in gebruikers/applicaties, statistieken, visibillity & control, trendanalyse.

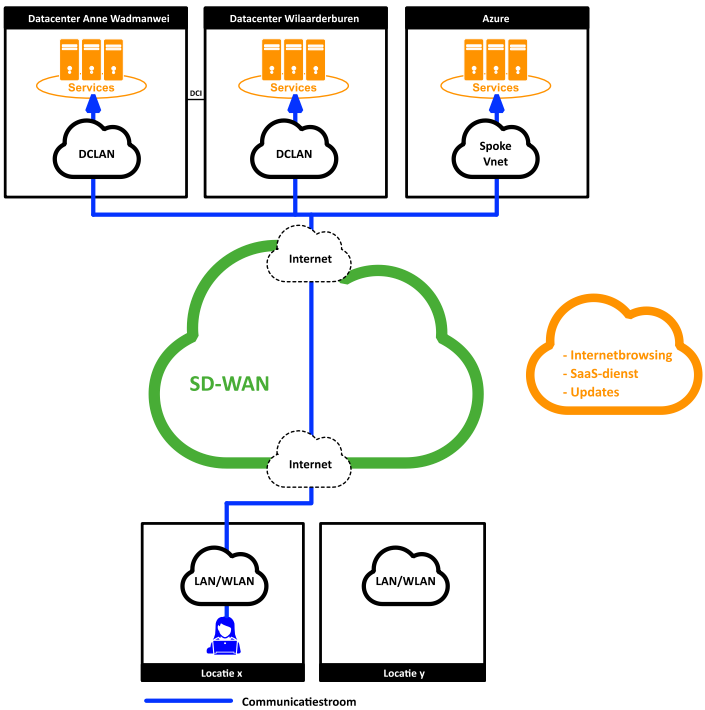
In de figuren 3-4 en 3-5 zijn communicatiestromen afgebeeld om dit concept illustratief te duiden.



Figuur 3-4: Verkeersstromen als:

- Regulier internetbrowsen,
- Benaderen SaaS-diensten,
- Ophalen van updates,

worden via de DIA (local breakout) afgehandeld. Dit geldt ook voor verkeersstromen afkomstig vanaf het on-premises-datacenter. Hoewel hier hairpinning van verkeer geen rol speelt, is de communicatiestroom wel afgebeeld omdat deze hetzelfde stramien volgt als op de verschillende locatietypen.



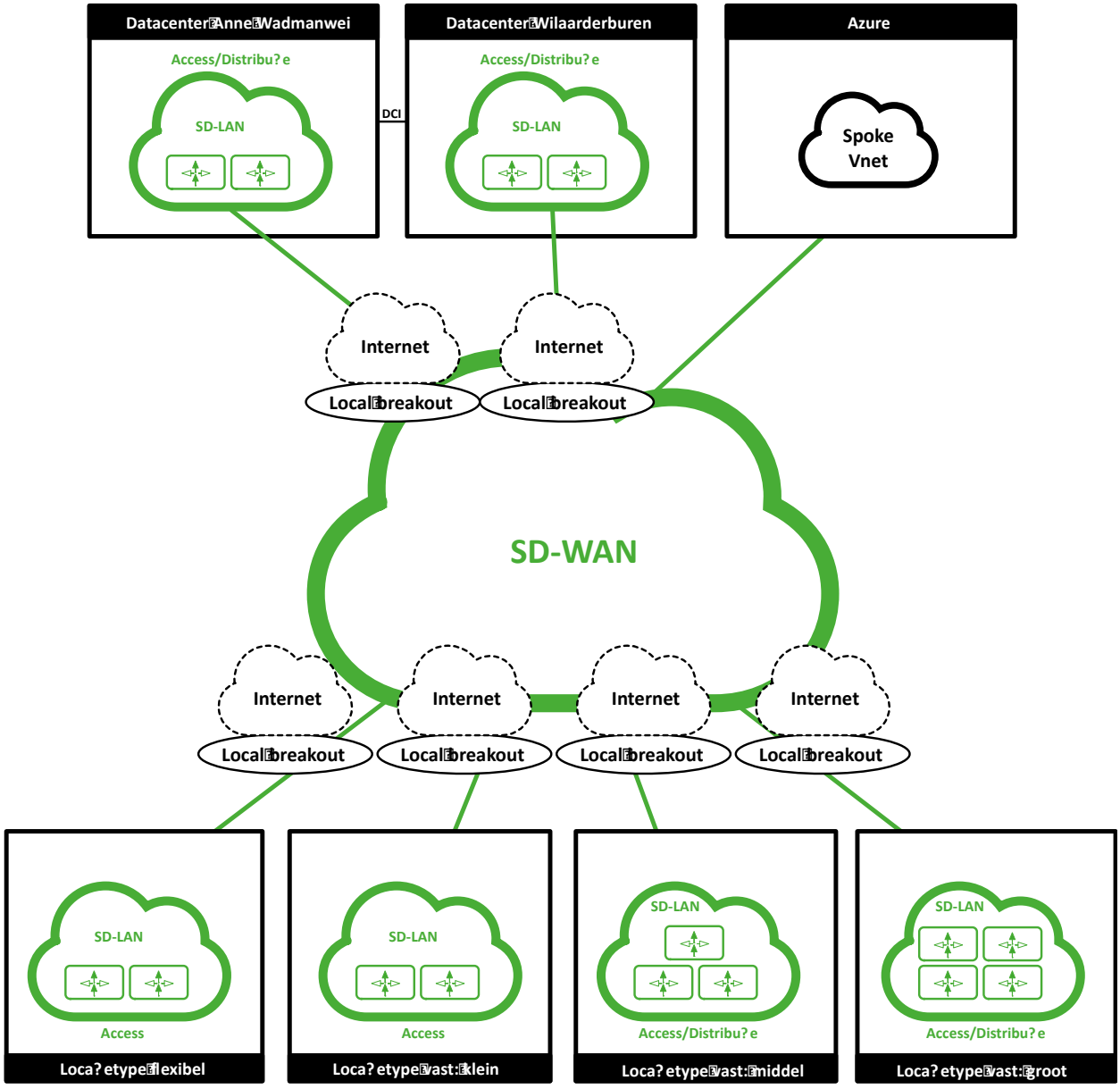
Figuur 3-5:
Andere verkeersstromen die als doel hebben services te gebruiken in het datacenter, maar ook vice versa (e.g. managementverkeersstromen vanuit het datacenter naar systemen/ componenten op de locatietypen van het ROC FP) maken gebruik van het SD-WAN met het internet als underlay-netwerk.

3.2.3.2 Technische eisen voor het SD-WAN

In bijlage 13e “Bijlage 13 E ROC FP Poortbezettingen dimensionering en SLA”, wordt per locatie de vereisten aangegeven van de WAN-ontsluiting, en de daarbij behoorde redunantie en SLA eisen.

3.2.4 SD-LAN

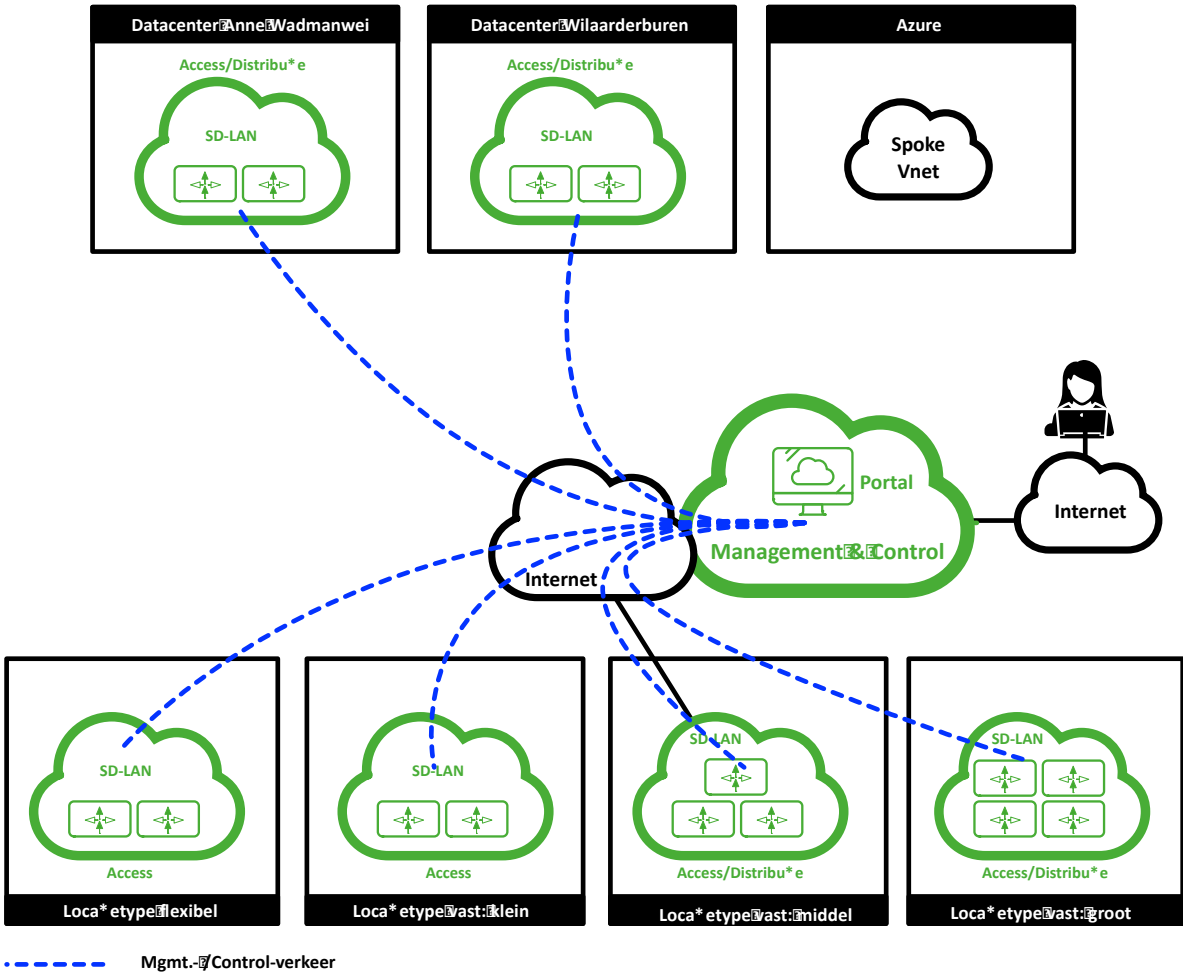
In de onderstaande illustratie is het SD-LAN high-level afgebeeld, waarbij wordt voortgeborduurd op de SD-WAN-beschrijvingen uit de vorige paragrafen. Dit om de SDN-stack end-to-end te duiden. Op grond van de ‘cloud, tenzij strategie’ van het ROC FP wordt uitgegaan van een controller als SaaS-dienst. Dit is in figuur 3-7 op de volgende pagina afgebeeld. Hiervan kan eventueel worden afgeweken, indien dit technologisch gezien een betere oplossing voortbrengt of waarbij het kostenaspect een andere oplossing dan een cloudoplossing rechtvaardigt. Kosten voor de oplossing (al dan niet als SaaS-dienst) behoren tot de NAAS-dienstverlening. De onderstaande figuur bevat derhalve dan ook de local breakout functionaliteit die in de paragraaf over het SD-WAN is beschreven.



Figuur 3-6: *Overzicht SD-LAN*

SD-LAN is een application & policy architectuur die hardware- en softwarelagen van elkaar scheidt en tegelijkertijd centraal beheerde netwerken realiseert die eenvoudiger te managen, te integreren en op- of af te schalen zijn. SD-LAN maakt hierbij gebruik van SDN-technologie en NFV (network function virtualisation) in de accesslaag. Deze accesslaag bevat componenten (i.e. LAN-switches) waarmee apparaten van eindgebruikers (e.g. laptops, desktops, servers) verbinding kunnen maken met het netwerk. Eindgebruikers zijn niet alleen personen met apparaten, maar ook bijvoorbeeld serversystemen. Derhalve wordt de SD-LAN-technologie ingezet op de verschillende locatietypen alsmede in het on-premises-datacenter (zoals afgebeeld in de illustratie). Opgemerkt moet worden, dat de Azure-omgeving hierin geen rol speelt. Binnen deze omgeving wordt in ieder geval geen SD-LAN-technologie ingezet die aanwezig is op de locatietypen en on-premises-datacenters van het ROC FP.

Het SD-LAN-concept biedt een netwerkbrede en op policies gebaseerde methode voor het beheer van apparaten in het LAN. De controllerfunctie (en managementfunctie) is ondergebracht in de cloud en de dataplane-functie is ondergebracht in de fysieke hardware op locatie. Deze centrale functionaliteit is afgebeeld in de onderstaande illustratie. Middels het internet staan de SD-LAN-nodes in contact met de centrale management- en controleromgeving die vanuit de cloud worden aangeboden.



Figuur 3-7: *Mgmt. en controleverkeer*

Middels de controller worden policies toegewezen aan alle apparaten in de accesslaag. Door deze centrale benadering/centraal concept wordt de provisioning van netwerknodes versneld en het beheer van de SD-LAN-omgeving gecentraliseerd. De centrale controller bewaakt continu de aangesloten apparaten en gebruikt policies om deze apparaten in staat te stellen te reageren op specifieke omstandigheden.

Door het gebruik van SD-LAN-technologie ontstaat zodoende betere/meer controle over het netwerk (tot aan de applicatielaag) en een beter/dieper inzicht in de prestaties en het gebruik van het netwerk.

3.2.4.1 Kenmerken van SD-LAN (i.e. functies die ondersteund worden)

Applicatie-optimalisatie

Het gedrag van het netwerk verandert dynamisch op basis van applicatieprioriteiten/SLA's. Door gebruik te maken van de centrale controllerfunctionaliteit ontstaat een fijnmazig inzicht in en zichtbaarheid/ controle over applicaties aan de randen van het netwerk.

Identity driven policies

Op basis van policies en context wordt toegang verleend (of ingetrokken) tot hetgeen gebruikers/ apparaten mogen doen/benaderen zodra deze zijn aangemeld op het SD-LAN-netwerk. Hierbij is het mogelijk policies in de controller aan te maken met als parameters 'type apparaat', 'type gebruiker/gebruikersgroep', 'type locatie', 'beschikbare bandbreedte', 'tijd van de dag'. Dit identity driven paradigma wordt ook wel intent based networking genoemd. Hierbij gaat het dus om de intentie die een gebruiker/applicatie heeft op het netwerk. Iedere applicatie en gebruiker worden eerst geïdentificeerd op het netwerk (i.e. middels NAC) om vervolgens op basis van profielen de aangemaakte policies toe te passen.

Gebruiker/applicatie visibility & control

De SD-LAN-componenten synchroniseren de data met de controller in de cloud (i.e. middels streaming telemetrie). Hierdoor is het mogelijk real-time inzicht in het gedrag van applicaties en gebruikers te krijgen. De controller maakt hierbij gebruik van Artificial Intelligence/Machine Learning om deze telemetrische gegevens te interpreteren en te correleren. Door gebruik te maken van Artificial Intelligence/Machine Learning wordt real-time inzicht in de gehele infrastructuur verkregen. Tevens kan op gebruikersniveau worden ingezoomd. Issues in het netwerk worden visueel zichtbaar gemaakt via de portal, waardoor efficiënt kan worden getroubleshoot. De cloudoplossing voorziet in ketenanalyse van een issue en stelt oplossingen voor op grond van best-practices.

Integratie SD-LAN/WiFi

Voor een end-to-end-inzicht in applicaties/gebruikers is het van belang, dat SD-LAN en het WiFi-netwerk integreren tot één unified access laag met gedeelde policies en management. Idealiter behoort integratie met het SD-WAN eveneens tot de mogelijkheden, waarbij alle functies van SDN middels de centrale cloudomgeving samenkomen voor een optimaal end-to-end-inzicht in gebruikers/applicaties, statistieken, visibillity & control.

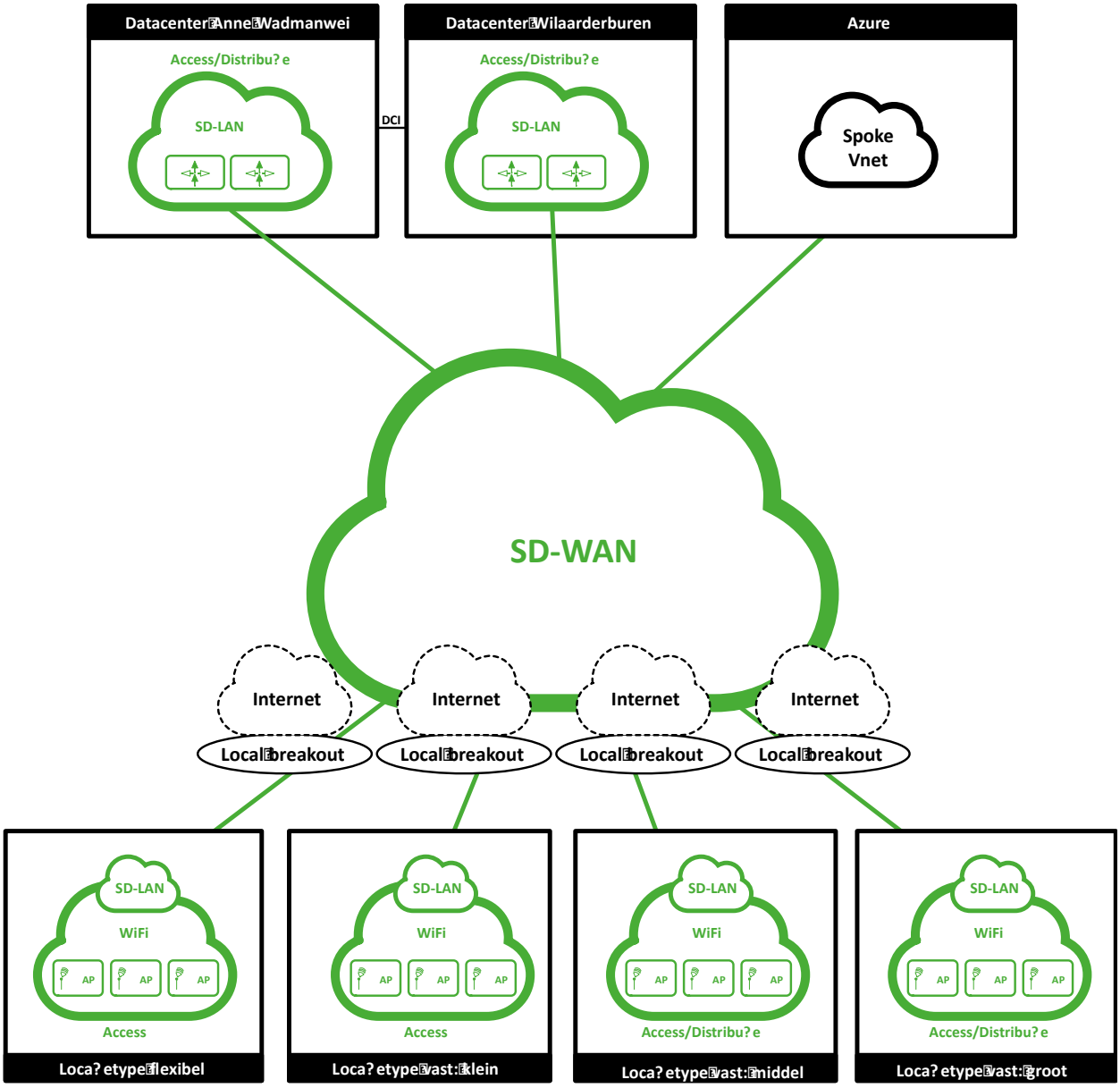
3.2.4.2 Technische eisen voor het SD-LAN

In bijlage 13e "Bijlage 13 E ROC FP Poortbezettingen dimensionering en SLA", wordt de poortomvang voor de accesslaag en de daaraan gestelde eisen beschreven voor de patchkasten van de verschillende locaties. In deze bijlage wordt aangegeven wat de huidige capaciteit is, en wat het geschatte huidige gebruik is. Deze schatting is gebaseerd op een rapportage van unclaimed ports in de maand februari. De aangeboden poortcapaciteit per patchkast moet 10% hoger liggen dan het geschatte gebruik op basis van de rapportage in februari. Ook wordt in deze bijlage per locatie een aantal poorten aangegeven, die

beschikbaar moeten zijn voor serverdiensten op de locatie. Voorbeeld hiervan is een server die images en applicaties aanbiedt voor het imageproces. Dit is dus additioneel aan de overige access-poorten.

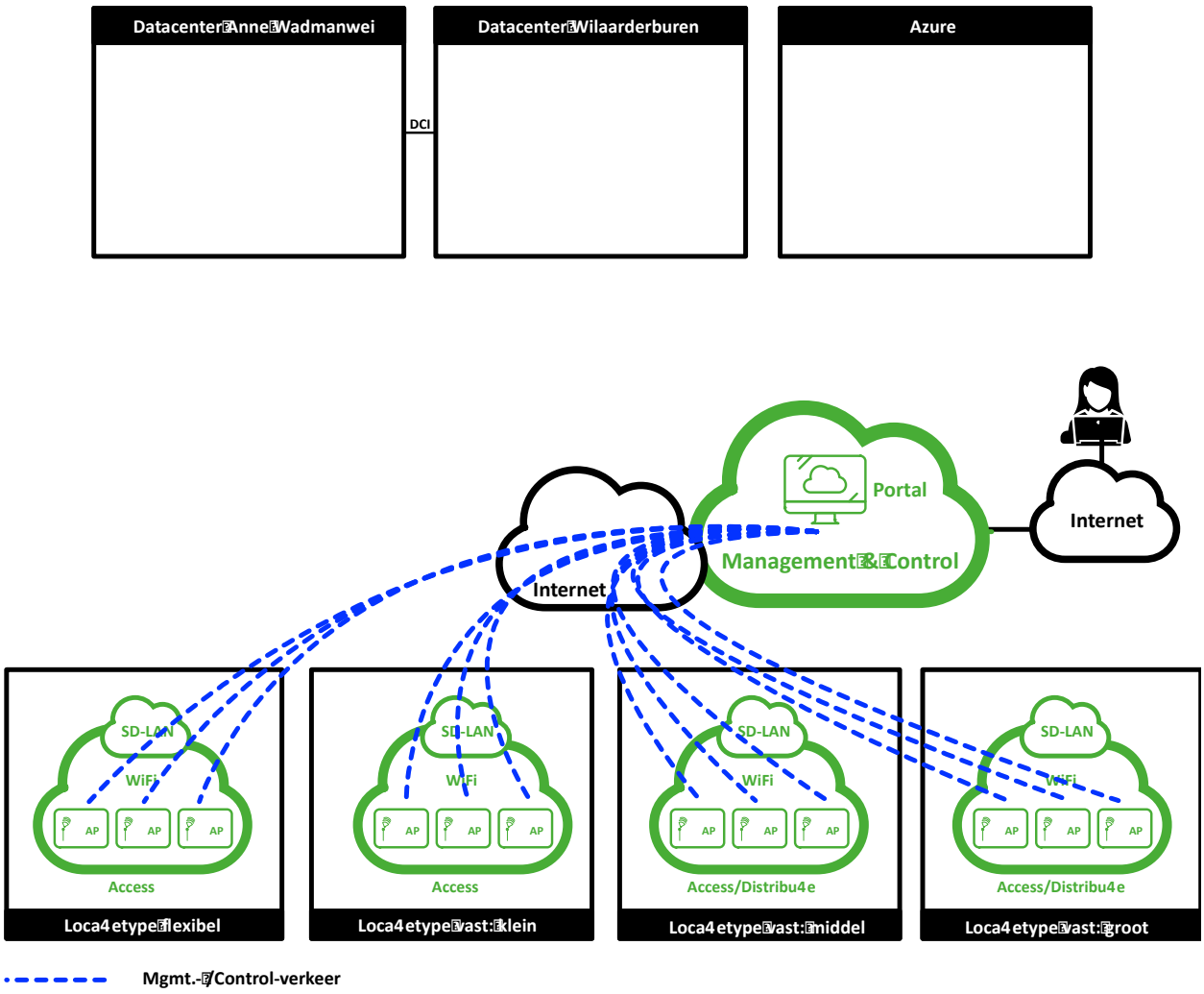
3.2.5 Wireless

In de onderstaande illustratie is het WiFi-netwerk high-level afgebeeld, waarbij wordt voortgeborduurd op de SD-WAN- en SD-LAN-beschrijvingen uit de vorige paragrafen. Dit om de SDN-stack end-to-end te duiden.



Figuur 3-8: *Overzicht WiFi-netwerk*

Op grond van de ‘cloud, tenzij strategie’ van het ROC FP wordt uitgegaan van een controller als SaaS-dienst. Dit is in figuur 3-9 afgebeeld. Hiervan kan eventueel worden afgeweken, indien dit technologisch gezien een betere oplossing voortbrengt of waarbij het kostenaspect een andere oplossing dan een cloudoplossing rechtvaardigt. Kosten voor de oplossing (al dan niet als SaaS-dienst) behoren tot de NAAS-dienstverlening. Figuur 3-8 bevat derhalve dan ook de local breakout functionaliteit die in de paragraaf over het SD-WAN is beschreven.



Figuur 3-9: *Mgmt. en controleverkeer*

De volgende SSID’s worden onderkend:

- Eduroam,
- Fp-portal,
- Fp-handheld.

Let op: Het ROC FP wil graag in overleg treden met de winnaar van de aanbesteding om toe te werken naar een oplossing met een beperkt aantal SSID's waarbij op basis van de gebruiker- en apparaat-authenticatie de gebruiker bepaalde functionaliteit krijgt toegewezen. Gezien een aantal beperkingen in de Eduroam 'standaard' kan ROC FP momenteel met Eduroam onvoldoende differentiëren tussen de verschillende devices in combinatie met de gebruiker.

3.2.5.1 Kenmerken van WiFi (i.e. functies die ondersteund worden)

Gecentraliseerd cloud managementplatform (webportal)

In figuur 3-9 is te zien, dat het management/controle van het WiFi-netwerk wordt gerealiseerd vanuit de cloud op grond van de 'cloud, tenzij strategie'. Zodoende is er on-premises geen controllerhardware of beheersoftware geïnstalleerd die onderhouden dient te worden. Alle software en firmware (beveiligings)updates worden vanuit de cloud geleverd als SaaS-dienst. De cloudoplossing heeft hiertoe ingebouwde tools voor troubleshooting op afstand. Op grond van deze 'cloud, tenzij strategie' wordt uitgegaan van een controller als SaaS-dienst. Hiervan kan eventueel worden afgeweken, indien dit technologisch gezien een betere oplossing voortbrengt of waarbij het kostenaspect een andere oplossing dan een cloudoplossing rechtvaardigt. Kosten voor de oplossing (al dan niet als SaaS-dienst) behoren tot de NAAS-dienstverlening.

Locatie Analytics (webportal)

Met Location Analytics worden realtime locatiestatistieken van de draadloze clients weergegeven. De access points verzamelen deze gegevens en synchroniseren deze met het cloudplatform. Middels de portal kunnen dashboards worden uitgelezen waarmee trends in bezoekersverkeer, actuele status van draadloze clients en nieuwe versus terugkerende draadloze clients e.d. kunnen worden achterhaald. Rapportages kunnen hierbij worden samengesteld met bijvoorbeeld historische gegevens van het WiFi-gebruik. Het is hierbij mogelijk het gedrag van gebruikers te simuleren en de reactiesnelheden van applicaties, WAN en het lokale netwerk te monitoren. Hierbij is het van belang te voldoen aan de AVG-verplichtingen die t.a.v. een onderwijsinstelling als het ROC FP gelden.

Application visibility & control

Via de portal is het mogelijk om inzicht te krijgen in applicaties en applicatieve verkeersstromen die gebruik maken van het WiFi-netwerk. Verkeersstromen kunnen hierbij worden geïnspecteerd en geclassificeerd, waarbij automatisch wordt vastgesteld of deze voldoen aan de vastgestelde Quality of Service parameters en SLA's. Er kan hierbij automatisch prioriteit verleend worden aan kritieke applicaties zoals VoIP, terwijl andere applicaties worden beperkt of geblokkeerd conform policies die centraal zijn belegd in de portal. Het is hierbij ook mogelijk applicaties en gebruikers die de meeste bandbreedte verbruiken te identificeren en middels traffic shaping policies te beperken in termen van bandbreedteconsumptie.

Door gebruik te maken van Artificial Intelligence/Machine Learning wordt real-time inzicht in de gehele infrastructuur verkregen. Tevens kan op gebruikersniveau worden ingezoomd. Issues in het netwerk

worden visueel zichtbaar gemaakt via de portal, waardoor efficiënt kan worden getroubleshoot. De cloudoplossing voorziet in ketenanalyse van een issue en stelt oplossingen voor op grond van best-practices.

Automatische RF-optimalisatie

De WiFi-configuratie is in staat om continu en automatisch de omgeving 'te monitoren' om zodoende de WiFi-prestaties te maximaliseren. Dit wordt gerealiseerd door het 'meten' van het kanaalgebruik, de signaalsterkte, doorvoersnelheden en het achterhalen van signalen van andere (interfererende) WiFi-componenten (e.g. real-time spectrum analysis and live channel utilization).

WiFi 6 (high capacity)

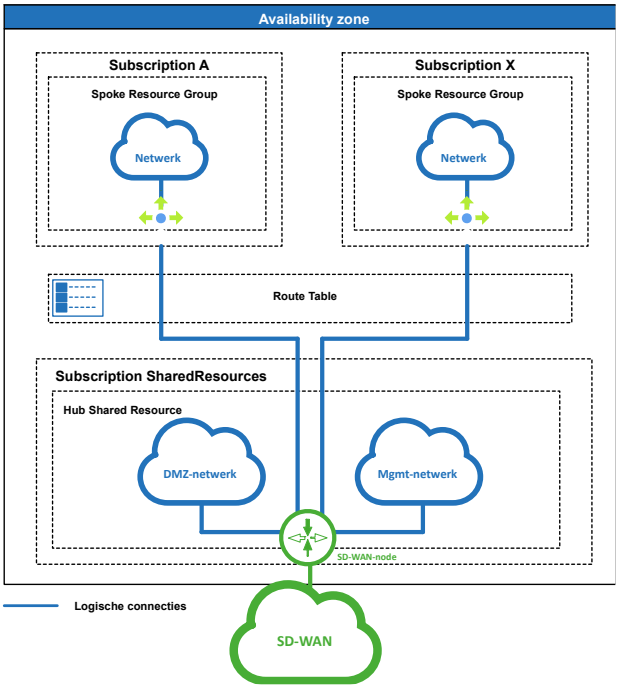
WiFi 6 is de opvolger van de standaard 802.11ac Wave 2 en heeft 3-4 keer betere/efficiëntere prestaties. De WiFi-configuratie is derhalve gebaseerd op minimaal deze nieuwe standaard, waarbij WiFi 6e tot de mogelijkheden behoort als dat passend is binnen een omgeving als het ROC FP.

Integratie SD-LAN/WiFi

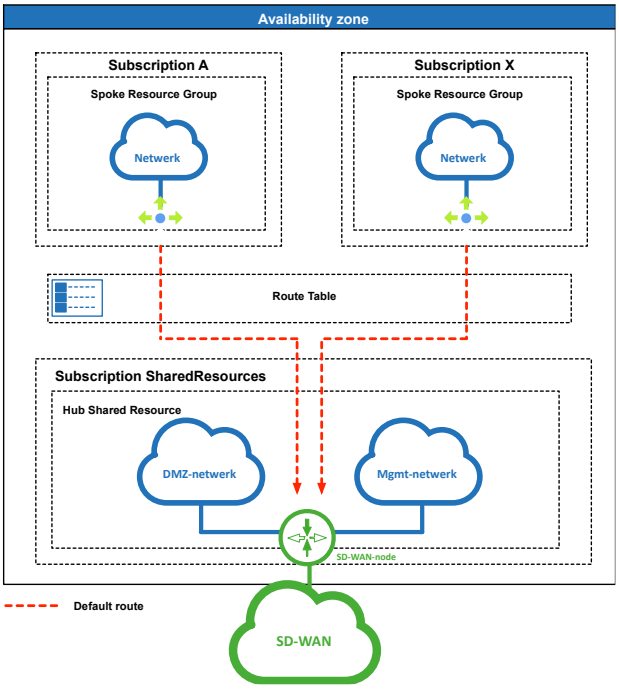
Voor een end-to-end-inzicht in applicaties/gebruikers is het van belang, dat het WiFi-netwerk en de SD-LAN-omgeving integreren tot één unified access laag met gedeelde policies en management. Idealiter behoort integratie met het SD-WAN eveneens tot de mogelijkheden, waarbij alle functies van SDN middels de centrale cloudomgeving samenkomen voor een optimaal end-to-end-inzicht in gebruikers/applicaties, statistieken, visibillity & control.

3.2.6 Azure

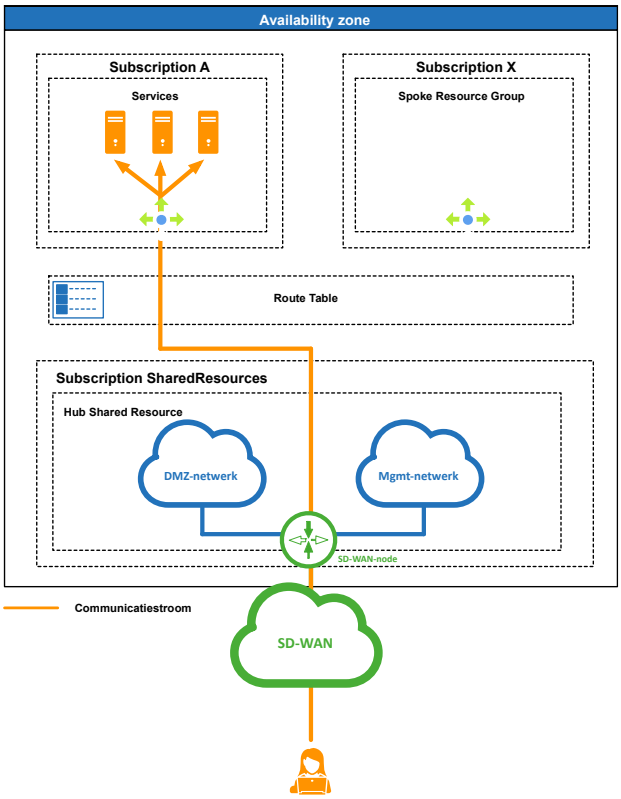
Het ROC maakt gebruik van Azure als clouddatacenter. Om de netwerkfuncties te duiden zijn in deze paragraaf een aantal illustraties opgenomen met tekst en uitleg.



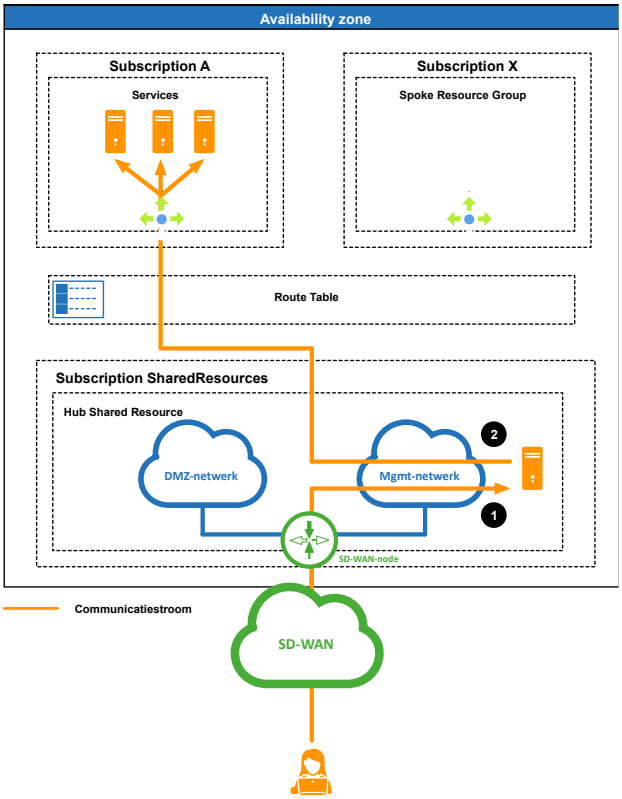
Figuur 3-10:
Azure wordt ook ontsloten middels het SD-WAN en wel voor IaaS-diensten die via het WAN benaderd dienen te worden. De SD-WAN-node wordt hierbij ondergebracht in de hub die shared resources bevat. Binnen het hubnetwerk zijn twee subnetten aangebracht: DMZ-netwerk en management-netwerk. De SD-WAN-node zelf wordt in een apart gateway subnet ondergebracht (derde subnet binnen de hub). Binnen de tenant zijn ook spoke-netwerk aangebracht waarbij per spoke een loadbalancer aanwezig is. De routetabel zorgt voor het begeleiden van verkeersstromen tussen de hub- en spoke-netwerken en naar het SD-WAN/internet.



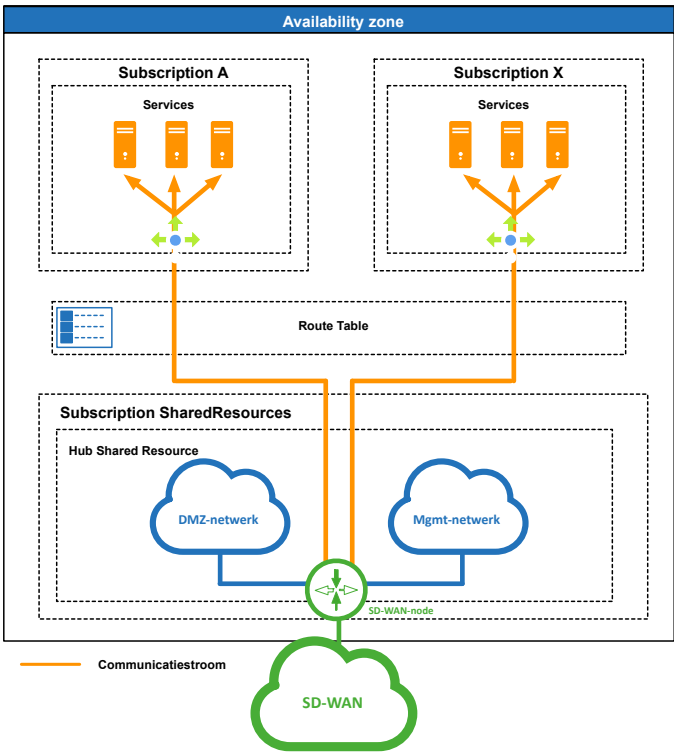
Figuur 3-11:
Verkeersstromen worden gedwongen via het hubnetwerk te verlopen alwaar de SD-WAN-node met PEP-functies is aangebracht. Zie par. 3.2.10 voor meer informatie over PEP-functies. De routetabel verzorgt in dit kader de default route middels UDR. Met andere woorden: systeemroutes van Azure worden hierbij overschreven. Immers, al het verkeer dient via de hub (SD-WAN-node) te verlopen waar het verkeersstromen betreft naar het internet, het SD-WAN-netwerk en tussen spokes. Verkeer binnen spokes kan binnen een spoke zelf worden afgehandeld mits de betreffende systemen/applicaties tot dezelfde zone behoren. Zie voor zonering par. 3.2.8.



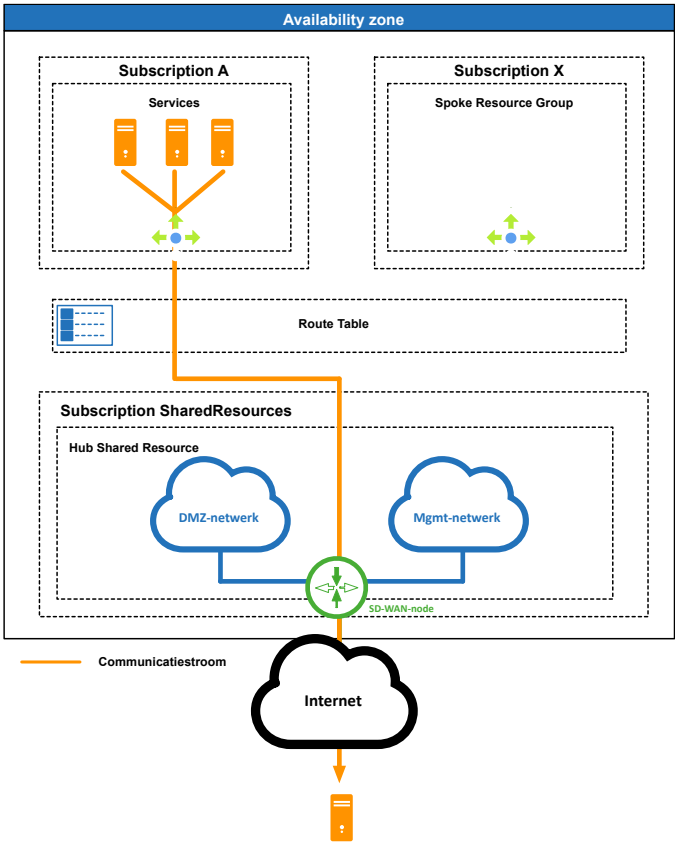
Figuur 3-12:
In de illustratie is een verkeersstroom afgebeeld afkomstig van een gebruiker op een bepaald locatietype. De verkeersstroom wordt via het SD-WAN getransporteerd naar de betreffende applicatie/systeem binnen een spoke-netwerk. Afhankelijk van de betreffende applicatie/systeem wordt wel/geen gebruikgemaakt van de loadbalancer.



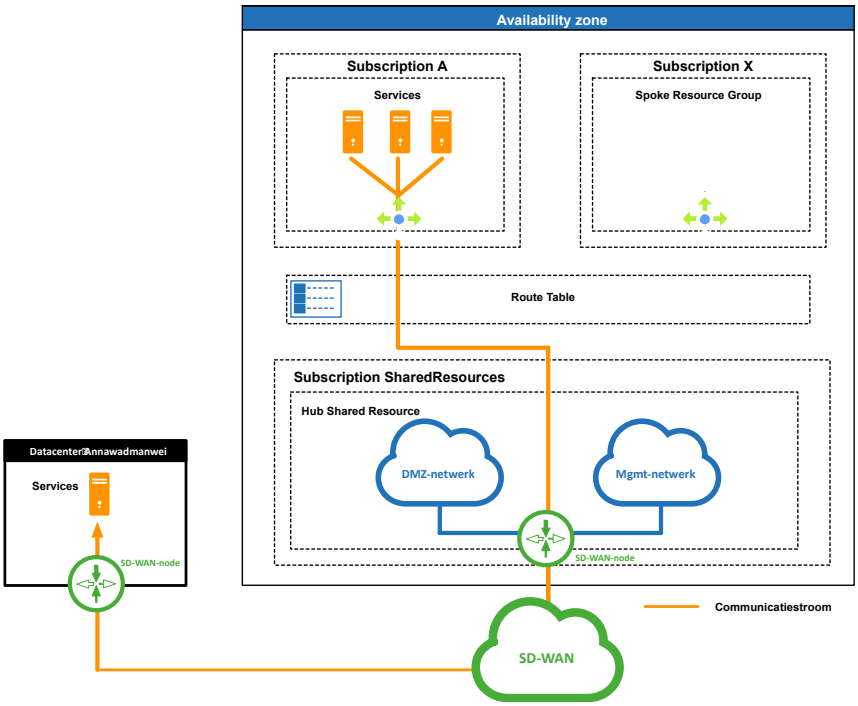
Figuur 3-13:
In deze figuur zijn verkeersstromen afgebeeld waarbij gebruikgemaakt wordt van een bastion host/jump server die zich in het managementnetwerk bevindt. Nr 1 duidt hierbij de communicatiestroom vanaf een type locatie naar de bastion host/jump server. Nr. 2 duidt het verdere verloop van de communicatie-stroom vanaf de bastion host/jump server. Let op: het dient ook mogelijk te zijn de bastion host/jump server vanaf het internet te kunnen benaderen indien een medewerker vanaf huis werkt.



Figuur 3-14:
Deze illustratie duidt de verkeersstroom tussen verschillende applicaties/systemen binnen verschillende spokenetwerken. Spoke-spoke-communicatie geschiedt te allen tijde via de hub (i.e. SD-WAN-node), ook al zijn de systemen in dezelfde zone opgenomen. Dit om ervoor te zorgen, dat geen directe spoke-vnet-spoke-vnet-connectie hoeft te worden aangemaakt, aangezien het ROC het hub-spoke-model volgt zonder uitzonderingen te hoeven maken. Uitzonderingen leiden immers tot potentiële fouten in de beheersystematiek.



Figuur 3-15:
In deze illustratie is communicatie afgebeeld tussen applicaties/systemen in een spoke-vnet en bijvoorbeeld een update-server op het internet. Communicatie wordt hierbij gedwongen te verlopen via het hubnetwerk (i.e. via de SD-WAN-node waar een local internet breakout aanwezig is).



Figuur 3-16:
In deze illustratie is communicatie afgebeeld tussen applicaties/ systemen in een spoke-vnet en services in het on-premises-datacenter. Communicatie wordt hierbij gedwongen te verlopen via het hubnetwerk (i.e. via de SD-WAN-node).

3.2.7 IoT

Stel je eens een wereld voor waar zowat alles wat je maar kunt bedenken online is en communiceert met andere ‘dingen’ en mensen om nieuwe diensten mogelijk te maken die ons leven verbeteren. Van zelfrijdende ‘drones’ die je boodschappen bezorgen tot sensoren in je kleding die je gezondheid monitoren, de wereld die we kennen zal een grote technologische verschuiving ondergaan. Deze verschuiving staat bekend als IoT, oftewel Internet of Things.

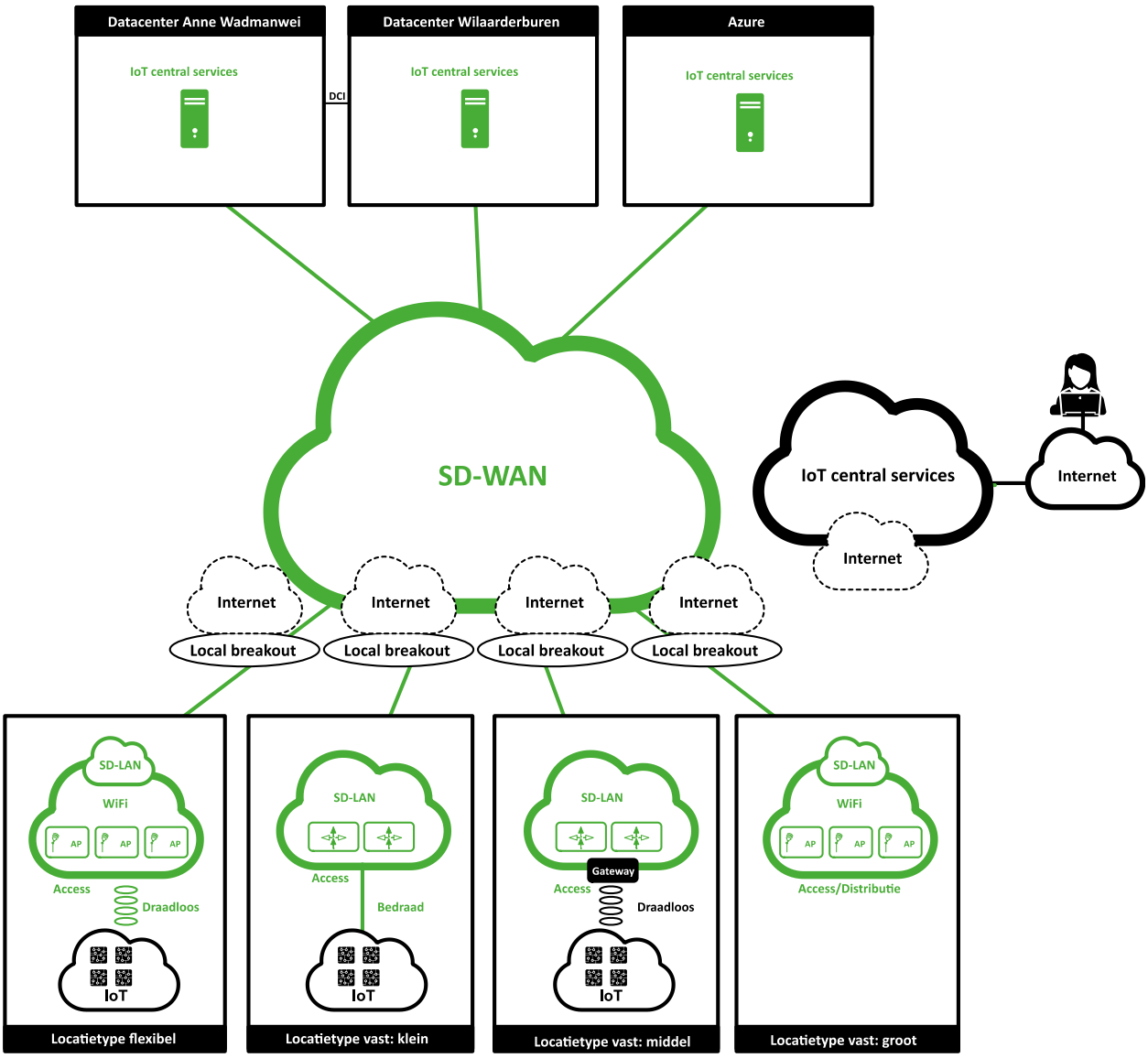
Het uitgangspunt en doel van IoT is om ‘de niet-verbonden objecten met elkaar te verbinden’. Dit betekent, dat objecten die momenteel niet zijn aangesloten op een computernetwerk (e.g. het internet) alsnog worden verbonden zodat deze kunnen communiceren met mensen en andere objecten. IoT is een technologische transitie waarbij apparaten ons in staat stellen de fysieke wereld als het ware ‘te voelen’ en te controleren door objecten slimmer te maken door deze te verbinden via een netwerk (e.g. het internet).

Wanneer objecten via een netwerk op afstand kunnen worden gedetecteerd en bestuurd, wordt een nauwere integratie tussen de fysieke wereld en computers mogelijk gemaakt. Dit zorgt voor verbeteringen op het gebied van efficiëntie, nauwkeurigheid, automatisering en het mogelijk kunnen maken van geavanceerde toepassingen.

De wereld van IoT is breed en veelzijdig en relatief complex vanwege de overvloed aan componenten en protocollen die het omvat. In plaats van IoT als een separaat technologiedomein te beschouwen, is het goed om het te zien als een paraplu met verschillende concepten, protocollen en technologieën die soms enigszins afhankelijk zijn van een bepaalde sector. Hoewel het brede scala aan IoT-elementen is ontworpen om tal van voordelen te creëren op het gebied van productiviteit en automatisering, introduceert het tegelijkertijd nieuwe uitdagingen, zoals het schalen van het enorme aantal apparaten, de hoeveelheden gegevens die moeten worden verwerkt en de beveiliging die hiermee gepaard gaat.

Ook binnen een scholengemeenschap als het ROC FP wordt in toenemende mate gebruikgemaakt van IoT-devices. Denk hierbij bijvoorbeeld aan IoT-devices in het educatieve domein (e.g. lasrobots, CNC-banken, 3D-printers), het facilitaire/administratieve domein (e.g. kassa’s, pinautomaten, alarmsystemen), het educatieve IT-domein (e.g. kweekkassen, scheepsimulatoren, Nikoservers) en toekomstige domeinen (e.g. IoT-devices voor als internetradio’s, weerstations, camera’s op digiborden).

Met andere woorden: IoT is vollop in ontwikkeling, ook binnen het ROC FP. In figuur 3-17 is het IoT-concept afgebeeld in relatie tot het netwerk van het ROC FP. De facto zijn de posities afgebeeld waar IoT-onderdelen zijn ondergebracht en de omgevingen aangestipt die een relatie hebben met IoT.

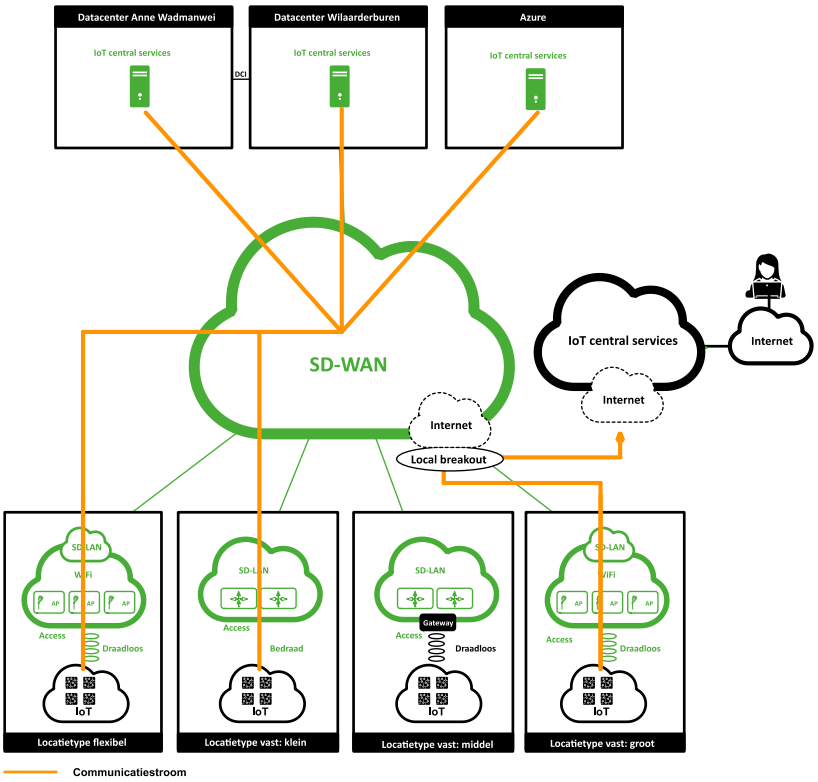


Figuur 3-17: *Overzicht IoT sensoren/devices en IoT central services*

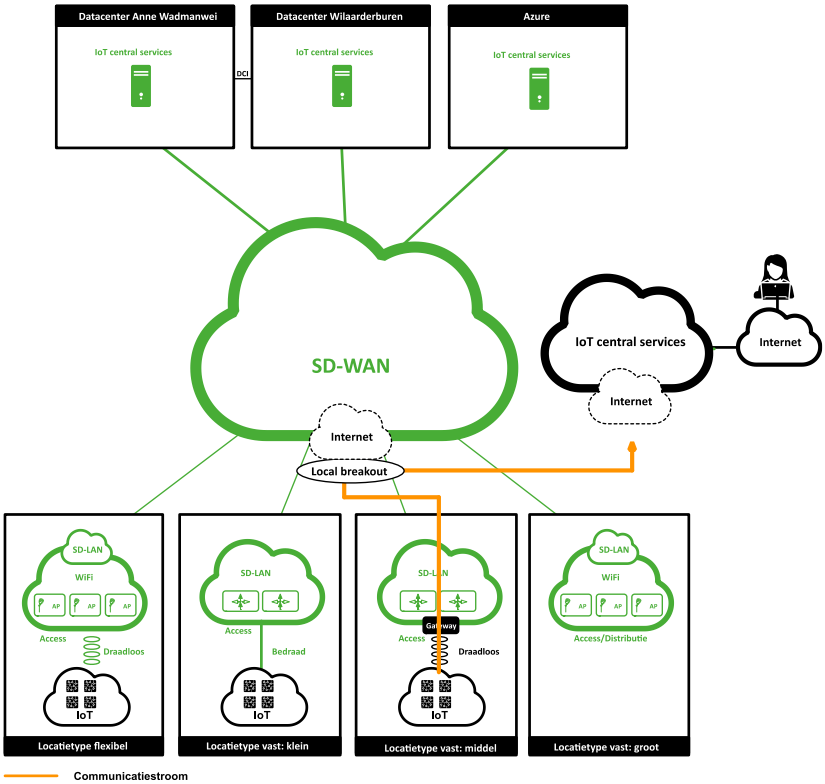
IoT-devices kunnen op 3 verschillende manieren worden ontsloten:

1. Via het draadloze netwerk (afgebeeld in het locatietype flexibel),
2. Via het bedrade netwerk (afgebeeld in het locatietype vast: klein),
3. Draadloos, gebruikmakend van een IoT gateway die bedraad is aangesloten (afgebeeld in het locatietype vast: middel).

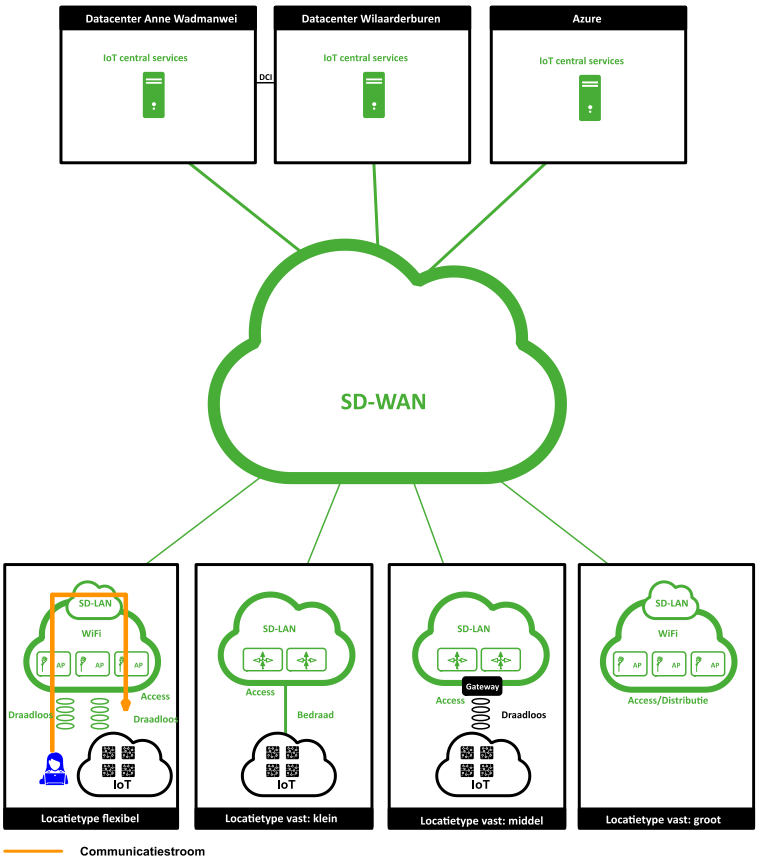
In de figuren op de volgende pagina's worden de communicatiestromen geduid die zich in het kader van IoT kunnen voordoen in het netwerk van het ROC FP.



Figuur 3-18:
In deze illustratie is communicatie afgebeeld tussen IoT-devices en centrale IoT services (e.g. IoT hubs, data-ontvangst). Via het SD-WAN verlopen communicatiestromen naar de on-premises-datacenters en het clouddatacenter Azure. Tevens is het mogelijk, dat IoT-devices gebruikmaken van de lokale internetuitbraak om direct het internet te bereiken (e.g. SaaS-dienst, regulier internet).



Figuur 3-19:
In deze illustratie is communicatie afgebeeld tussen de IoT gateway en de centrale IoT service. Dit scenario doet zich doorgaans voor bij SaaS-diensten en is derhalve op deze plaats opgenomen. Tevens is het mogelijk, dat een PaaS-dienst als IoT hub vanuit Azure wordt afgenomen. Dit impliceert dan ook een communicatiestroom die direct het internet benadert middels de lokale internetuitbraak.

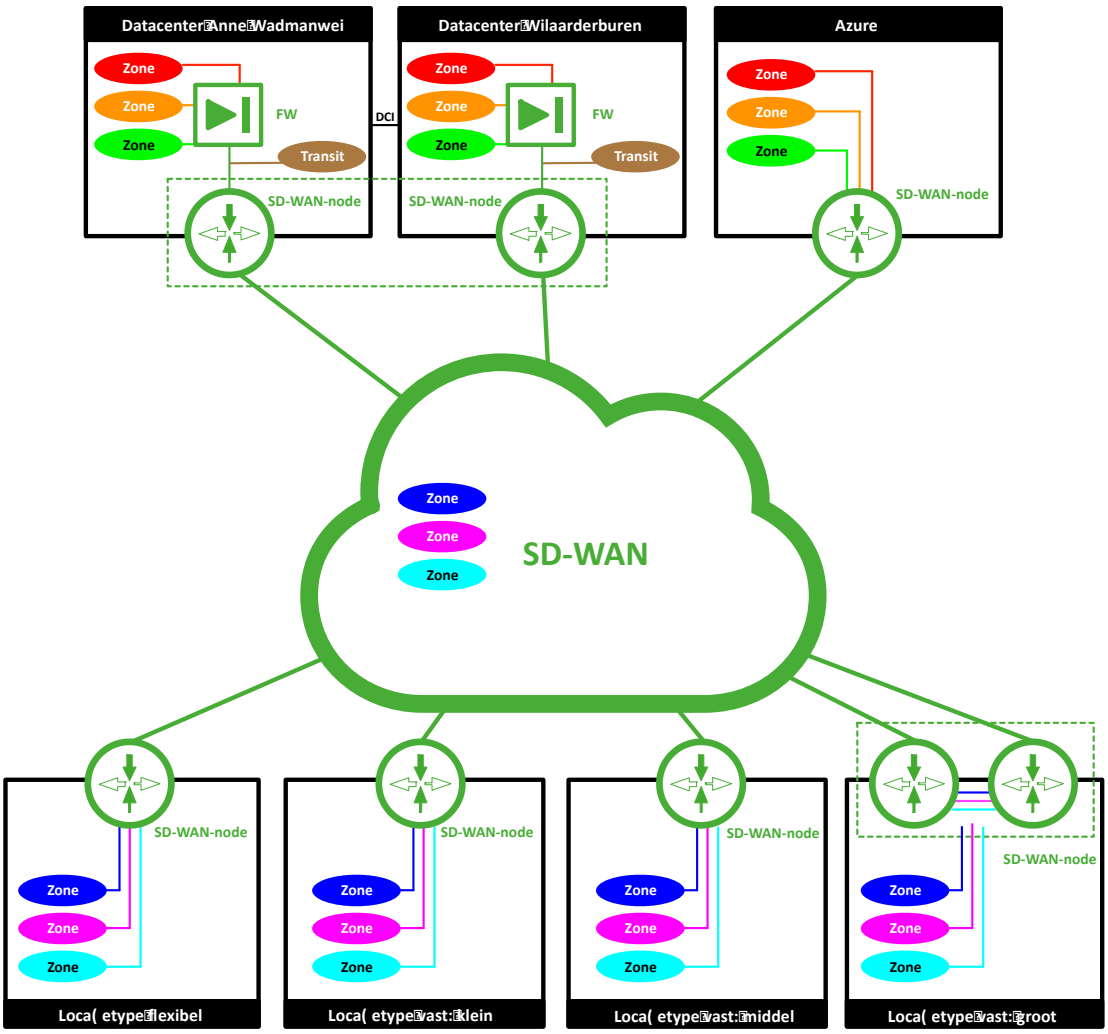


Figuur 3-20:
In deze illustratie is communicatie afgebeeld tussen gebruikers en IoT-devices op een locatie (e.g. denk aan scenario's voor educatieve doeleinden). De communicatie wordt hierbij afgehandeld via de combinatie WiFi/SD-LAN-netwerk.

3.2.8 Zonering/segmentatie

3.2.8.1 Zonering

Het beschouwingsmodel *zonering* is geënt op een categoriseringsmodel, waarbij een systeem- of gebruikersgroep met een bepaalde 'vertrouwdheid' wordt ondergebracht in een zone. Een zone is derhalve een groep IT-voorzieningen met dezelfde eigenschappen/kenmerken op het gebied van beveiliging, afgebakend door een deel van het netwerk. In theorie c.q. volgens de literatuur is binnen een zone onderlinge gegevensuitwisseling zonder meer mogelijk, waarbij gegevensuitwisseling tussen zones wordt gereguleerd door een beveiligingsfunctie (i.e. PEP-functie) als een filter/firewall[2]. Het primaire doel van zonering is het isoleren van risico's, zodat bedreigingen en incidenten in de ene zone niet doorwerken in de andere zone. De omgeving van het ROC FP is onderverdeeld in zones. In de onderstaande illustratie is dit zoneringsconcept high-level afgebeeld.



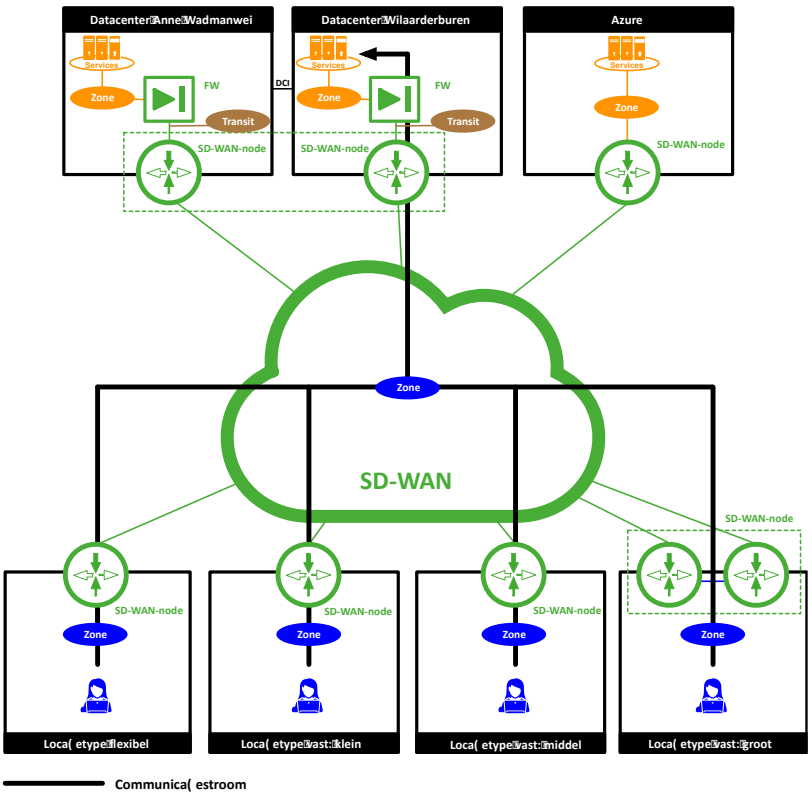
Figuur 3-21: *Zonering conceptueel*

[2] Denk aan het NORA-zoneringsmodel. Echter, in de praktijk van ROC FP zullen segmenten worden aangemaakt binnen zones, waarbij communicatie geschiedt op basis bepaalde communicatiemodellen die verderop worden beschreven.

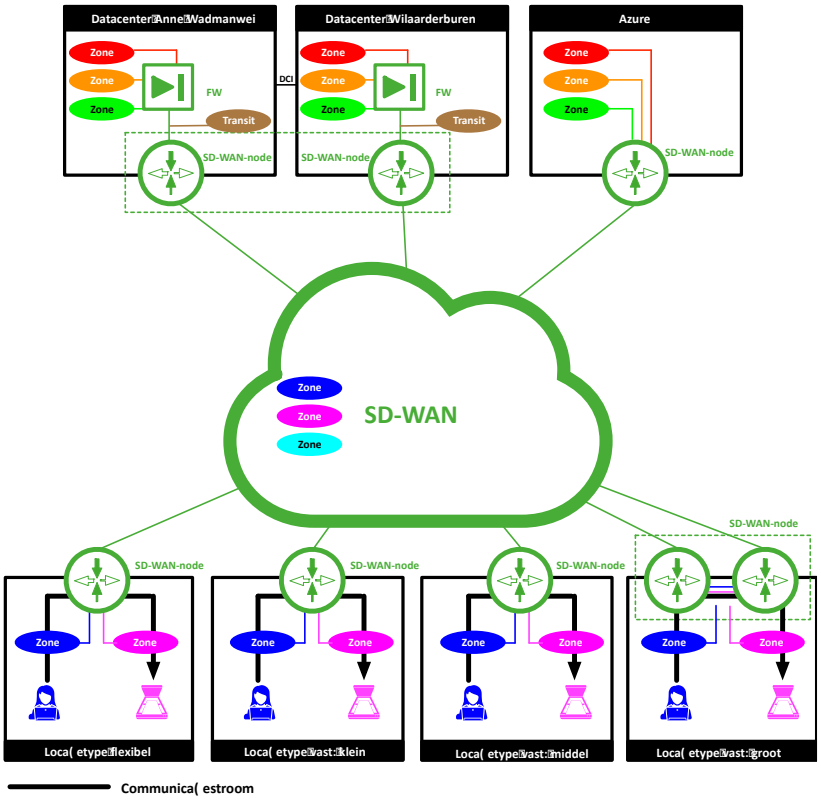
Zowel op het niveau van een locatietype (i.e. SD-LAN, WiFi), het SD-WAN, het on-premises datacenter (SD-LAN, firewall) als binnen de Azure-omgeving zijn zones aangebracht, specifiek voor ROC FP. De volgende zones worden hierbij onderkend (op hoofdlijnen).

Omgeving	Zones
Locatietypen	• Educatief, • Administratief, • Ondersteunend, • Management, • IoT, • Quarantaine, • Internet.
SD-WAN	• Educatief, • Administratief, • Ondersteunend, • Beheer, • IoT,
On-premises datacenter	• Internet, • DMZ, • Productie front-end, • Productie back-end • OTA front-end, • OTA back-end, • Beheer
Azure	• Internet, • DMZ, • Productie front-end, • Productie back-end • OTA front-end, • OTA back-end, • Beheer

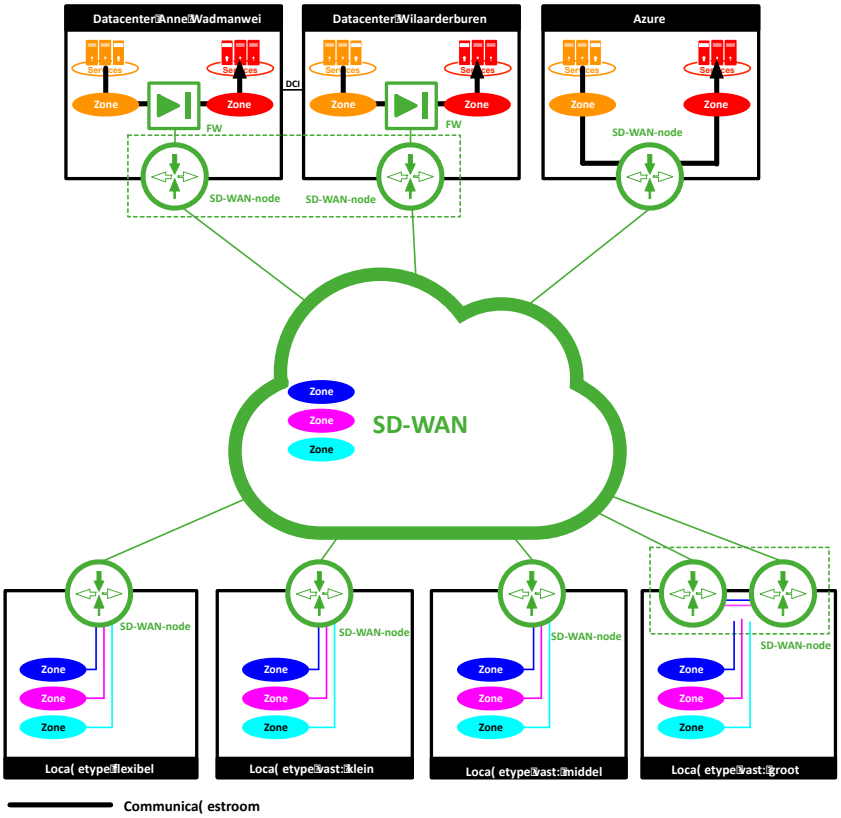
In de volgende illustraties zijn generieke verkeersstromen afgebeeld die end-to-end kunnen voorkomen in het netwerk van het ROC FP. De daadwerkelijke communicatiestromen (en toe te passen PEP-functies) dienen verder te worden uitgewerkt. Dit in overleg met de markt. Het is van belang, dat het netwerk van ROC FP de functionaliteit van zonering (en PEP-functies) i.i.g. ondersteunt.



Figuur 3-22:
In deze situatie benutten de gebruikers services vanuit het on-premises datacenter (of vanuit Azure, niet zijnde SaaS/PaaS-diensten die via het internet worden benaderd, maar IaaS-diensten). Tussen een locatietype en het SD-WAN wordt alleen de functie van statefull firewall gebruikt om ervoor te zorgen, dat alleen de vooraf gedefinieerde communicatie-stromen worden toegelaten. Tussen het SD-WAN en het datacenter worden PEP-functies toegepast (zone-overgangen -> blauw -> bruin -> oranje).



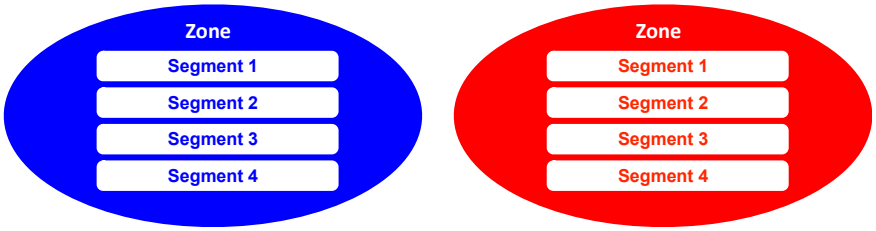
Figuur 3-23:
In deze situatie benutten de gebruikers services binnen een locatietype (e.g. printservice). Door de zone-overgang blauw -> paars dienen PEP-functies te worden toegepast.



Figuur 3-24:
In deze situatie is er communicatie tussen serversystemen in de on-premises datacenters en Azure (e.g. front-end back-end communicatie). Door de zone-overgangen oranje -> rood dienen PEP-functies te worden toegepast.

3.2.8.2 Segmentatie

Het aanbrengen van verschillende zones is een eerste stap in de richting van isolatie en gegevensafscherming. Om het beveiligingsniveau verder te verhogen worden segmenten aangebracht binnen een zone. Hierdoor is het mogelijk risico's verder te isoleren op het niveau van een zone. In de onderstaande illustratie is dit concept afgebeeld.



Figuur 3-25: *Segmenten binnen zones*

Om verkeersstromen in het netwerk te kunnen herleiden tot de zones en segmenten dienen deze eerst te worden vastgesteld. Een model dat hierbij helpt bestaat uit drie verschillende typen communicatiestromen:

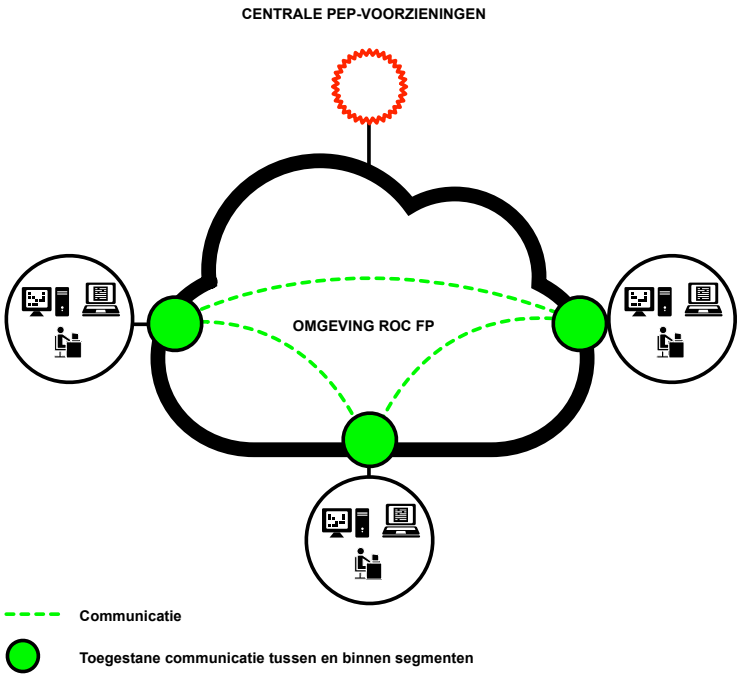
1. Non-secure,
2. Secure,
3. Secure private.

Iedere communicatiestroom heeft eigen karakteristieken in termen van:

- Toegestane verkeersstromen,
- PEP-functies (Policy Enforcement Point).

Model 1: Non-secure

Dit model heeft betrekking op 'reguliere segmenten', waarbinnen users/systemen elkaar direct kunnen benaderen zonder tussenkomst van PEP-functies die door de centrale PEP-voorzieningen worden uitgeoefend. De verkeersstroom wordt derhalve decentraal in het netwerk afgehandeld, waarbij directe communicatie zowel binnen hetzelfde segment als tussen verschillende segmenten is toegestaan. In de onderstaande illustratie is dit model conceptueel afgebeeld:



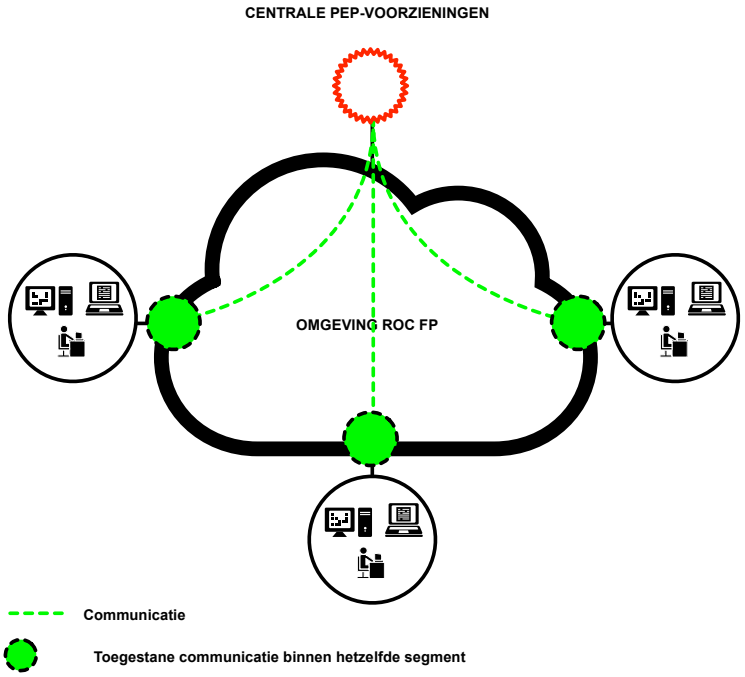
Figuur 3-26: *Model 1: non-secure segment*

Model 2: Secure

Dit model heeft betrekking op segmenten, waarbij:

- Binnen hetzelfde segment onderlinge communicatie is toegestaan. Users/systemen binnen hetzelfde segment kunnen zodoende elkaar direct benaderen, zonder tussenkomst van de centrale PEP-voorzieningen.
- De (on)mogelijkheid tot communicatie tussen verschillende segmenten in de centrale PEP-voorzieningen is aangebracht, zodat directe communicatie tussen verschillende segmenten niet mogelijk is maar door de PEP-functies wordt gereguleerd.

In de volgende illustratie is dit model afgebeeld:



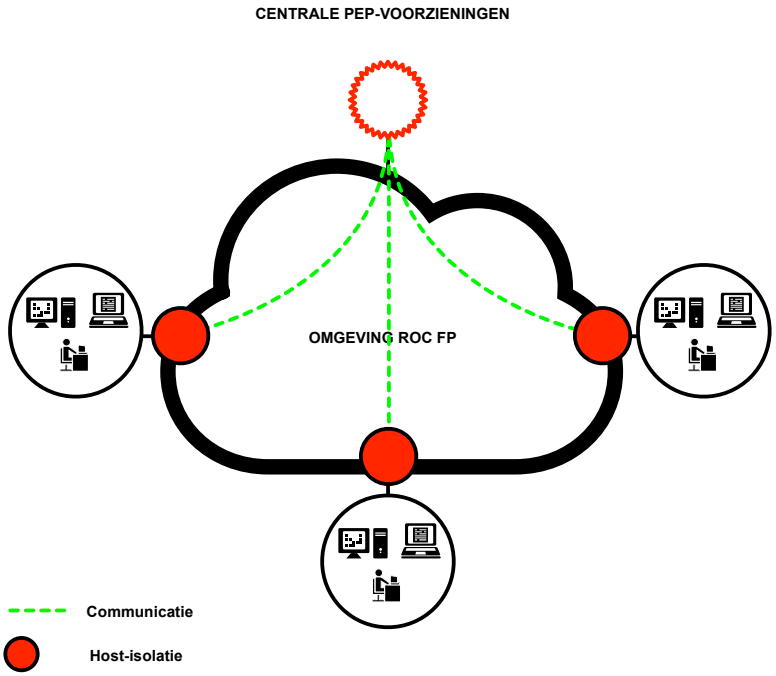
Figuur 3-27: *Model 2: Secure segment*

Model 3: Secure private

Dit model heeft betrekking op segmenten, waarbij:

- Onderlinge communicatie binnen hetzelfde segment niet is toegestaan. Users/systemen binnen hetzelfde segment kunnen elkaar **niet** direct benaderen (i.e.: host isolation),
- Communicatie tussen verschillende segmenten niet is toegestaan. Users/systemen binnen verschillende segmenten kunnen elkaar niet direct benaderen,
- De communicatiemogelijkheid in de centrale PEP-voorzieningen is aangebracht, zodat iedere vorm van onderlinge communicatie tussen users/systemen te allen tijde via deze PEP-functies plaatsheeft.

In de volgende illustratie is dit model afgebeeld:



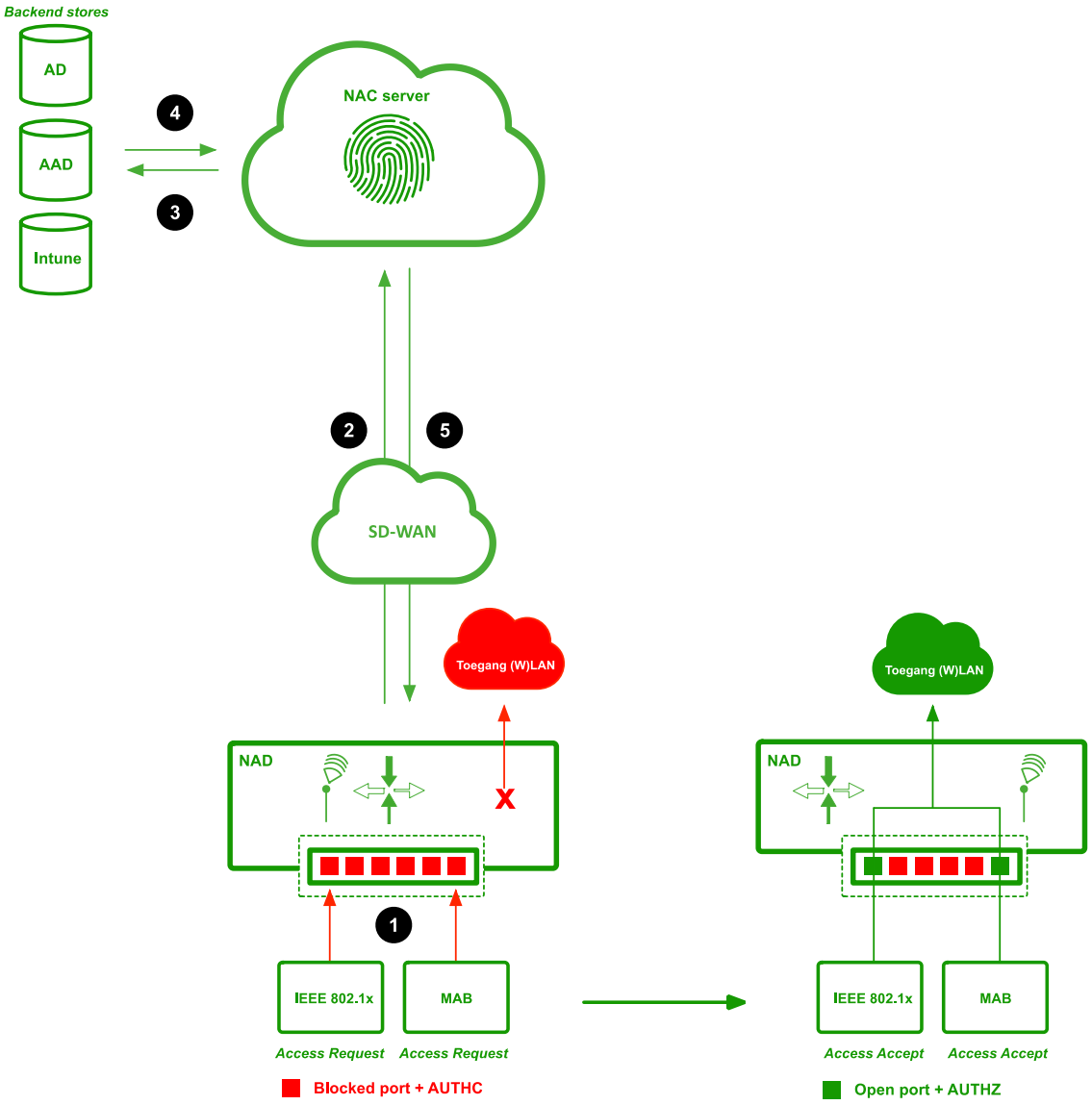
Figuur 3-28: *Model 3: Secure private*

Dit model is de facto gebaseerd op het zero-trust-concept met een netwerkgerelateerde vertaling in microsegmentatie.

3.2.9 Network Access Control (IEEE 802.1x/MAB)

3.2.9.1 Managed devices/CYOD

Om het netwerk en de services/resources van het ROC FP nog beter te beschermen wordt NAC (Network Access Control) toegepast in de accesslaag. Dit betreft zowel de bedrade als de draadloze accesslaag binnen de verschillende locatietypen. Een NAC-oplossing verleent gebruikers, computers en systemen op een gecontroleerde wijze toegang tot het netwerk. Het hart van een NAC-oplossing wordt gevormd door de Policy Server (RADIUS-server) die op basis van ROC FP-beleidsregels authenticaties en autorisaties voor gebruikers, computers en systemen doorvoert. In de onderstaande figuur is het concept NAC high-level afgebeeld.



Figuur 3-29: *NAC-oplossing high-level*

In de figuur is een aantal nummers opgenomen dat het proces van authenticatie en autorisatie high-level beschrijft:

Nr. 1 Access Request
Een entiteit als een medewerker met een door het ROC FP beheerde laptop/PC of een managed printer wil toegang tot het netwerk verkrijgen en initieert hiertoe communicatie met een NAD. Een NAD is een Network Access Device zoals een access switch of access point. De netwerkpoort of 'virtuele poort' (WiFi) is gesloten (niet geautoriseerd) en laat vooralsnog alleen IEEE 802.1x/MAB (MAC Address Bypass) verkeer door.

Nr. 2 RADIUS-sessie
Voordat een NAD toegang verleent tot het netwerk worden:

- de user credentials van een gebruiker,
- het computer account van de beheerde PC/laptop waarmee de gebruiker werkt,
- het MAC-adres van de printer,

middels het RADIUS-protocol verstuurt naar de NAC-oplossing die de sessie met credentials/MAC-adres doorzet naar de back-end stores voor validatie.

Nr. 3 Authenticatie (back-end stores)
Er zijn drie verschillende back-end stores binnen het ROC FP:

- Active Directory omgeving (voor managed computers die deel uitmaken van het AD-domein),
- Azure Active Directory (voor gebruikers en hybride joint managed computers),
- Intune voor CYOD (Choice Your Own Device) devices.

In de voorgaande omgevingen worden de gebruikers, managed computers, managed devices als printers geauthentiseerd.

Nr. 4 Autorisatie
Na succesvolle authenticatie bepaalt de Policy Server wat het autorisatieniveau van de betreffende gebruiker, managed laptop/PC, CYOD en printer is. Autorisatiekenmerken kunnen zijn: VLAN-toewijzing, downloadable ACLs waarmee gebruikers/systemen in bepaalde VLANs worden ondergebracht met beperkte toegang tot resources middels de dACLs, tags die door het gehele netwerk van ROC FP gebruikt kunnen worden voor het toepassen van policies e.d.

Nr. 5 Access Accept
Na succesvol te zijn geauthentiseerd en geautoriseerd verstuurt de Policy Server middels het RADIUS-protocol de juiste instellingen naar de NAD die de gebruiker, managed laptop/PC, CYOD-device en printer toegang verleent tot het netwerk (bedraad of draadloos). In de rechterzijde van de illustratie is

dit conceptueel afgebeeld. De poort is geopend met een bepaald autorisatieprofiel (AUTHZ) in tegenstelling tot de linkerzijde, waarin de poort is geblokkeerd opdat eerst authenticatie (AUTHC) dient plaats te hebben.

3.2.9.2 BYOD

De vraag naar een brede aanpak van BYOD wordt steeds groter en steeds sterker. Dit komt vanuit verschillende invalshoeken.

Vanuit het perspectief van studenten:

- Toename van studenten met een eigen device,
- Leren en samenwerken op andere plekken,
- Buiten de reguliere onderwijsvestigingen en locaties.

Vanuit het perspectief van ROC FP:

- Meer gebruik van digitaal lesmateriaal dat overal en op elk moment gebruikt kan worden,
- Onderwijsteams ICT, Uniform beroepen en Maatschappelijke Zorg maken gebruik van BYOD voor studenten,
- Flexibele moderne huisvesting, groei in gebruik digitale content en lesmethoden (blended learning),
- Uitstraling en imago van ‘moderne’ onderwijsinstelling.

Het gebruik van BYOD dient echter wel voldoende te zijn geborgd middels technische en beveiligingsfuncties. Zodra studenten/gastdocenten gebruik moeten maken van bijvoorbeeld IoT-services op de verschillende locatietypen, services die vanuit de centrale datacenters worden aangeboden of services die lokaal worden aangeboden, dient het betreffende BYOD-device te worden ‘geonboard’ via de BYOD-procedures van de Policy Server. Dit impliceert dat een ‘stukje software’ op het BYOD-device wordt ondergebracht waarmee het mogelijk is de status van het device te duiden in termen van compliancy (e.g. laatste virusupdates, laatste besturingsupdates, laatste software-updates et cetera). Met andere woorden: posture assessment wordt hierbij uitgevoerd. Indien een device niet compliant is, krijgt het alleen toegang tot de zone ‘quarantaine’ waarmee alleen het internet kan worden bereikt om alsnog middels remediation servers de laatste status van software, updates e.d. te downloaden. Hierna kan het device opnieuw proberen toegang te krijgen tot het netwerk van het ROC FP.

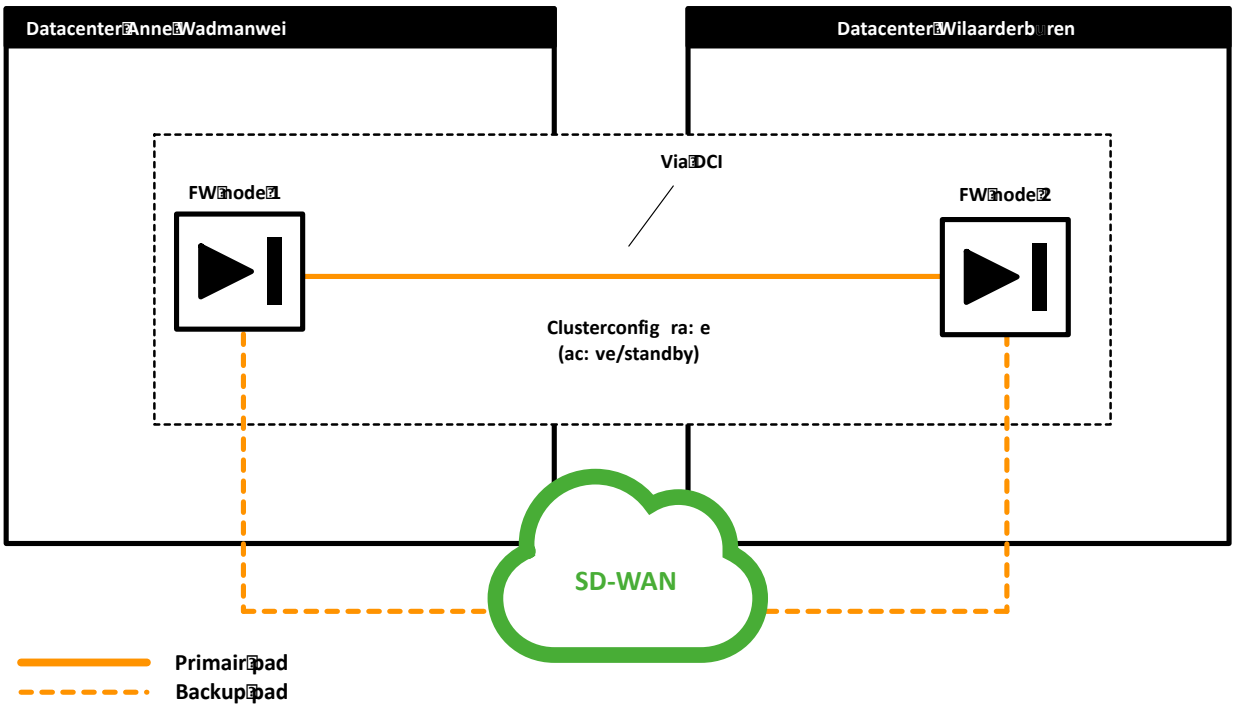
3.2.9.3 IoT

IoT devices krijgen waar mogelijk bij voorkeur toegang tot het netwerk via IEEE 802.1x. Indien dit niet mogelijk is kan worden volstaan met MAB.

3.2.10 PEP-functies

3.2.10.1 Centrale on-premises firewall

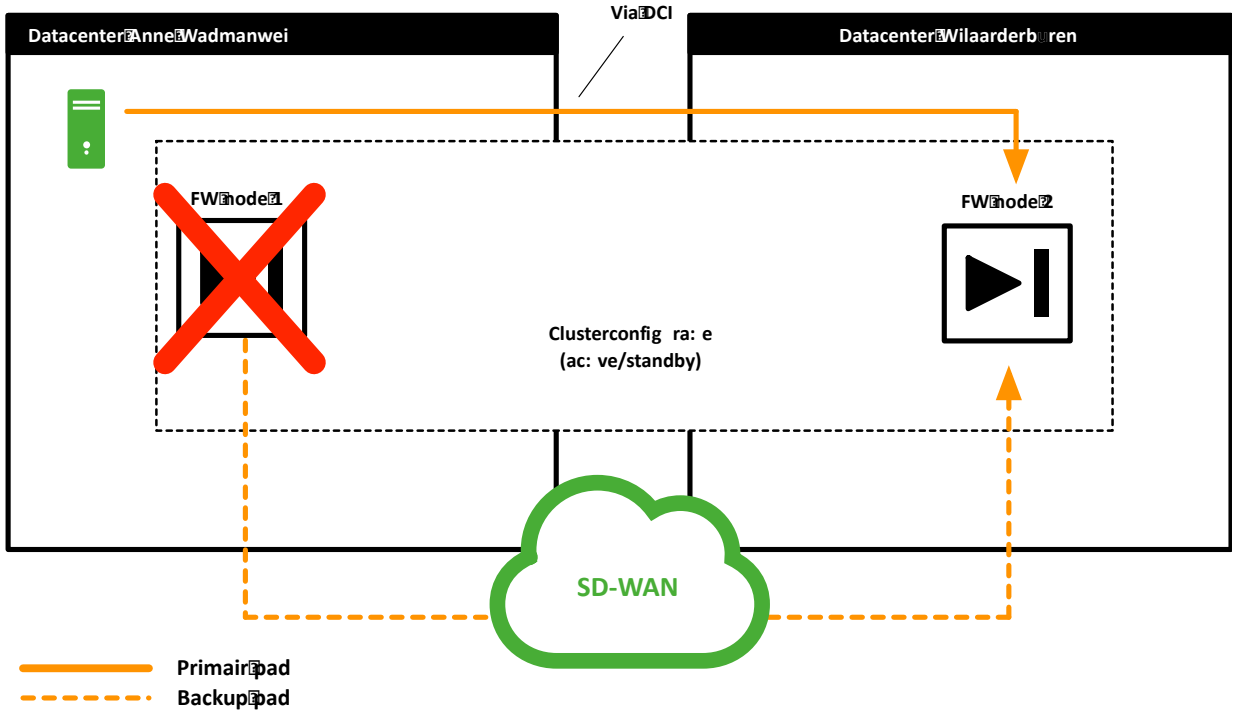
In het on-premises datacenter van ROC FP wordt per datacenter een firewallnode aangebracht. In de onderstaande illustratie is dit conceptueel afgebeeld.



Figuur 3-30: *Firewallnodes on-premises datacenter (incluis failover)*

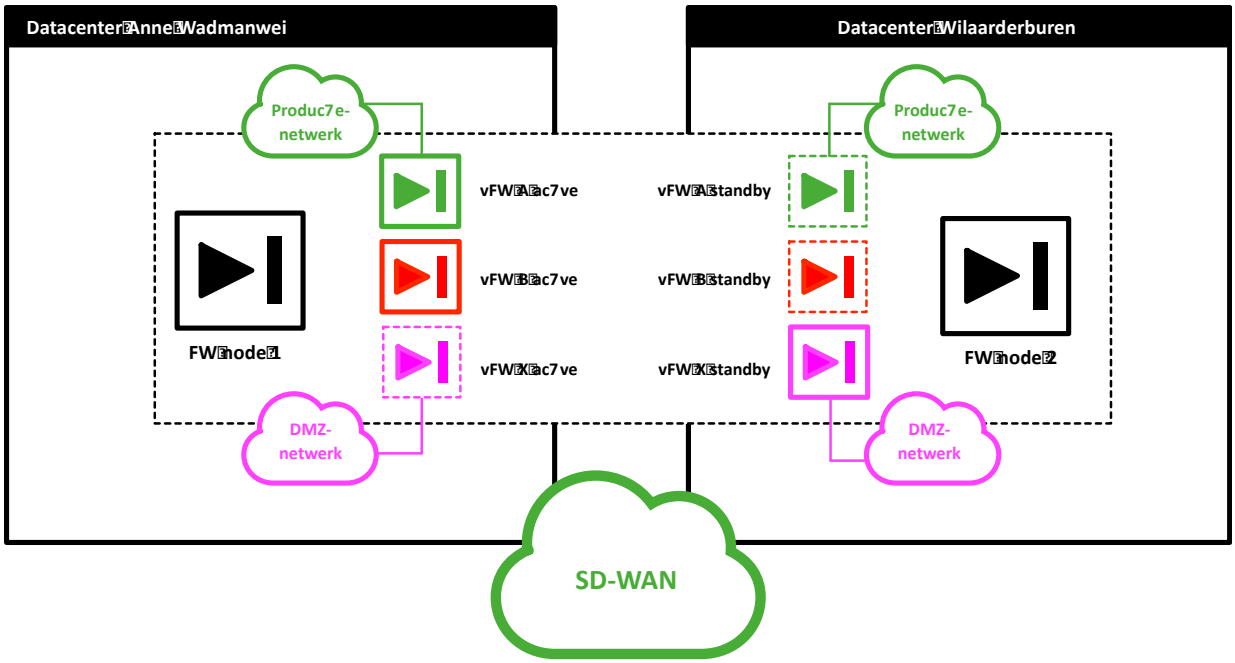
De bovenstaande illustratie geeft een active - standby cluster weer dat wordt gebouwd tussen de beide on-premises-datacenters. Tussen de nodes is communicatie noodzakelijk die ervoor zorgt, dat er geen split-brain-situatie ontstaat. Dit geschiedt middels de zogenaamde heart-beat-gegevensoverdracht tussen de nodes. Het is hierbij van belang, dat de communicatiestroom wordt afgehandeld middels de DCI (datacenter interconnect) die aanwezig is tussen de beide datacenters. Het SD-WAN-netwerk is hierbij het backup-pad indien door omstandigheden het DCI-netwerk niet meer functioneert.

Hetzelfde geldt voor verkeersstromen die door servers worden geïnitieerd of geretourneerd indien één van de firewall nodes (of één van de virtuele firewalls (zie verderop)) niet meer functioneert zoals in de volgende illustratie is geduid.



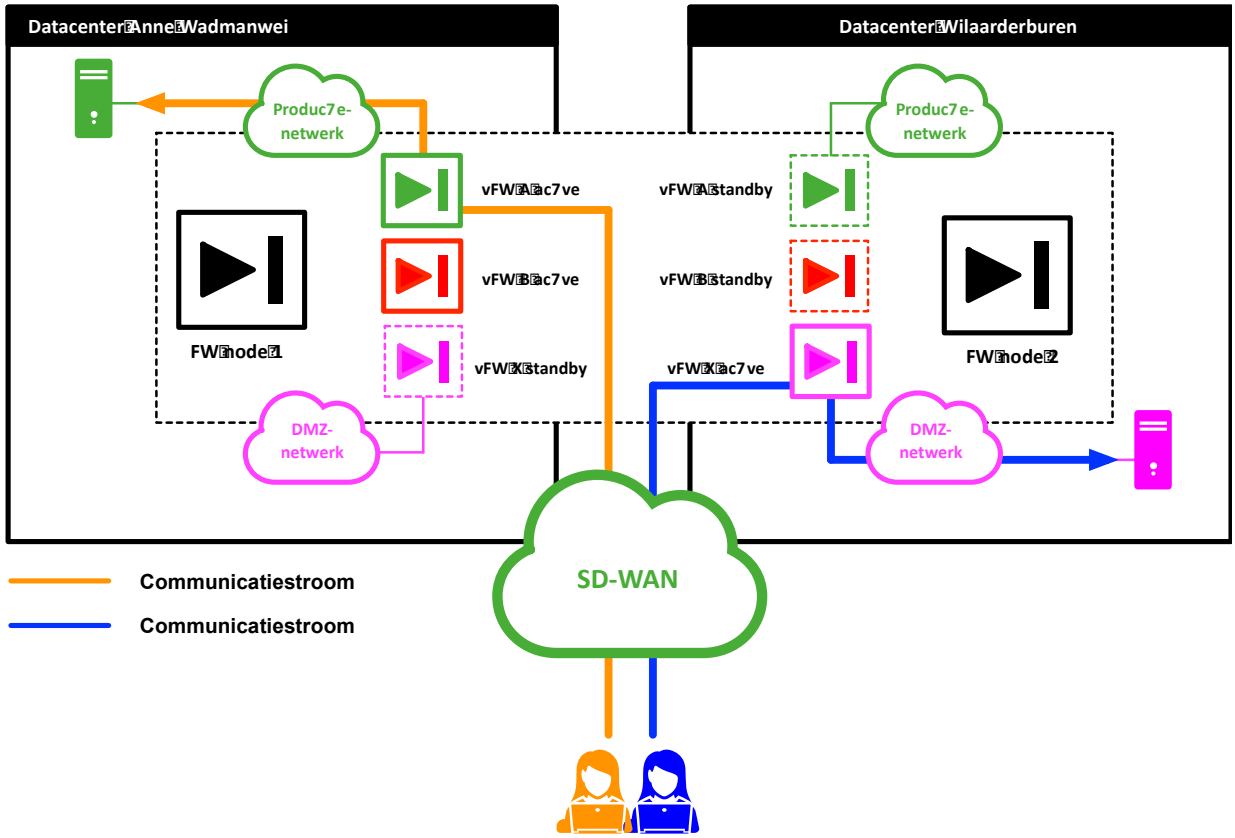
Figuur 3-31: *Failover firewallnodes on-premises datacenter*

De fysieke firewallnodes worden gevirtualiseerd in verschillende virtuele firewalls zoals in de onderstaande figuur conceptueel is afgebeeld.



Figuur 3-32: *Virtuele firewalls binnen de fysieke nodes*

De constellatie bestaat uit een active/standby concept dat is toegepast op de beide on-premises-datacenters. Hierbij kan de standby virtuele firewall automatisch actief worden, indien een issue zich voordoet in de primary firewall zoals afgebeeld in de onderstaande figuur.



Figuur 3-33: *Communicatiestromen bij uitval primaire virtuele firewall*

De virtuele firewalls volgen hetzelfde stramien als de fysieke nodes (vanuit het perspectief van het datacenter):

- Primaire communicatie via de datacenter interconnectie,
- Secundaire / backup communicatie via het SD-WAN-netwerk.

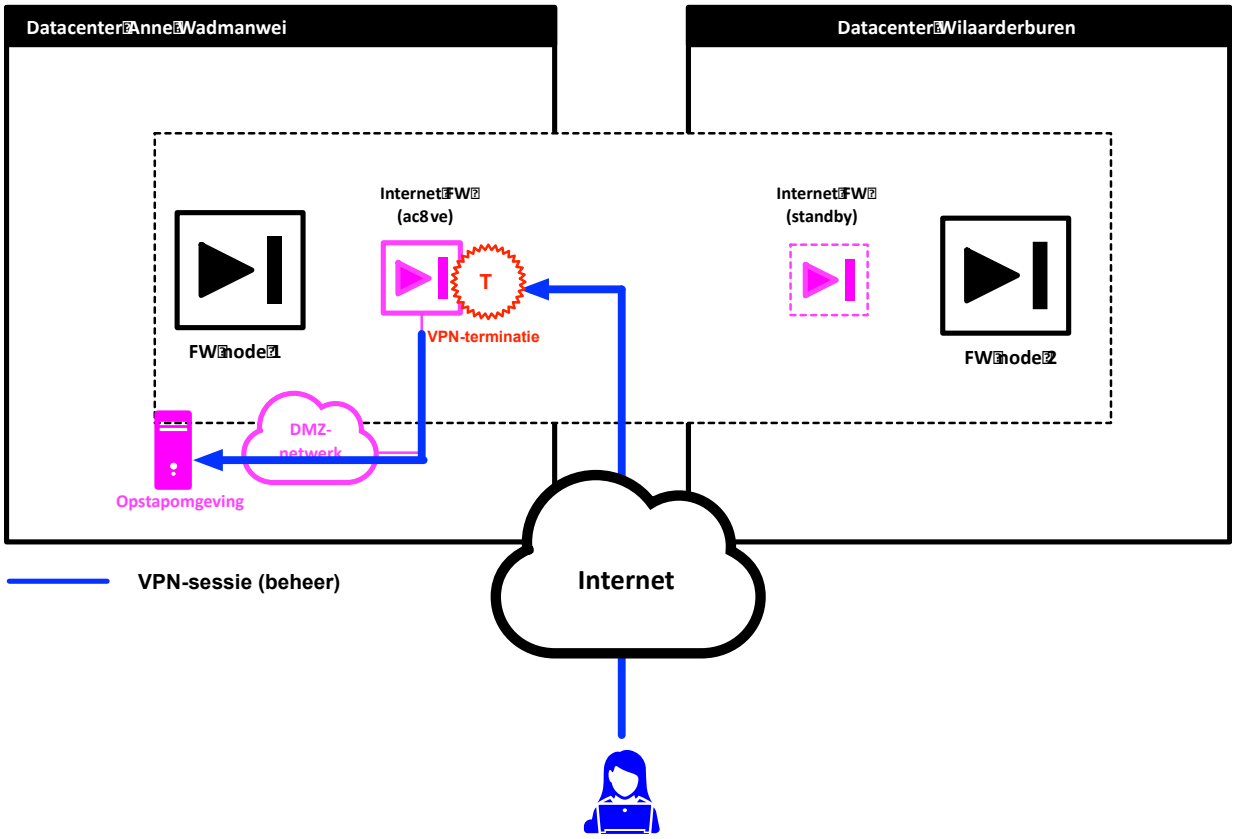
De volgende virtuele firewalls worden aangebracht:

- Internetfirewall,
- DMZ-firewall,
- Productiefirewall,
- OTA-firewall.

De firewall dient hierbij de volgende PEP-functies te ondersteunen[3]:

- E-mail filter,
- Zonering/segmentatie,
- VPN.

De firewall dient het gebruik van VPN te ondersteunen. Hoewel deze functie op de keper beschouwd geen Policy Enforcement Point is (maar wel binnen het VPN-concept PEP-functies kan toepassen (e.g. statefull firewalling, encryptie)), is in de onderstaande figuur het VPN-concept afgebeeld (client VPN, maar ook site-to-site-VPN's zijn in scope).



Figuur 3-34: *VPN-sessie, terminatie internet firewall*

[3] NAT en statefull firewalling zijn niet expliciet opgenomen. Deze functionaliteiten zijn inherent aan een firewall.

3.2.10.2 SD-WAN-niveau

Traditionele beveiligingsmodellen zijn ontworpen vanuit het perspectief, dat applicaties/systemen vanuit het on-premises-datacenter worden aangeboden. Er was zodoende alleen maar een centrale firewall die alle applicaties/systemen beschermde tegen aanvallen vanaf (voornamelijk) het internet. Echter, dit centrale firewallmodel is aan het verdwijnen door de 'cloudification' van applicaties/ systemen die vanaf gebruikerslocaties direct via het internet worden benaderd zonder hierbij middels hairpinning de centrale on-premises-datacenter te gebruiken. Met andere woorden, de centrale beveiligingsperimeter is aan het verdwijnen en wordt vervangen door beveiligingsparameters aan de edge van de infrastructuur.

Derhalve worden ook op het niveau van het SD-WAN PEP-functies aangebracht. Het is hierbij van belang, dat tussen de on-premises firewalls en de SD-WAN-nodes geen dubbele PEP-functies worden aangebracht. In dit HLD wordt uitgegaan van een minimalistische set aan PEP-functies op het niveau van de on-premises-firewalls en een volledige set aan PEP-functies op het niveau van het SD-WAN. De reden hiervoor is integraliteit van de oplossing, waarbij het SD-WAN op zowel decentraal niveau (i.e. locatietypen) als centraal niveau (i.e. on-premises-datacenter, Azure) een vitale beveiligingsrol vervult. Met andere woorden: er wordt getracht om punt-oplossingen/geïsoleerde oplossingen te voorkomen.

PEP-functies waarin het SD-WAN voorziet zijn de volgende:

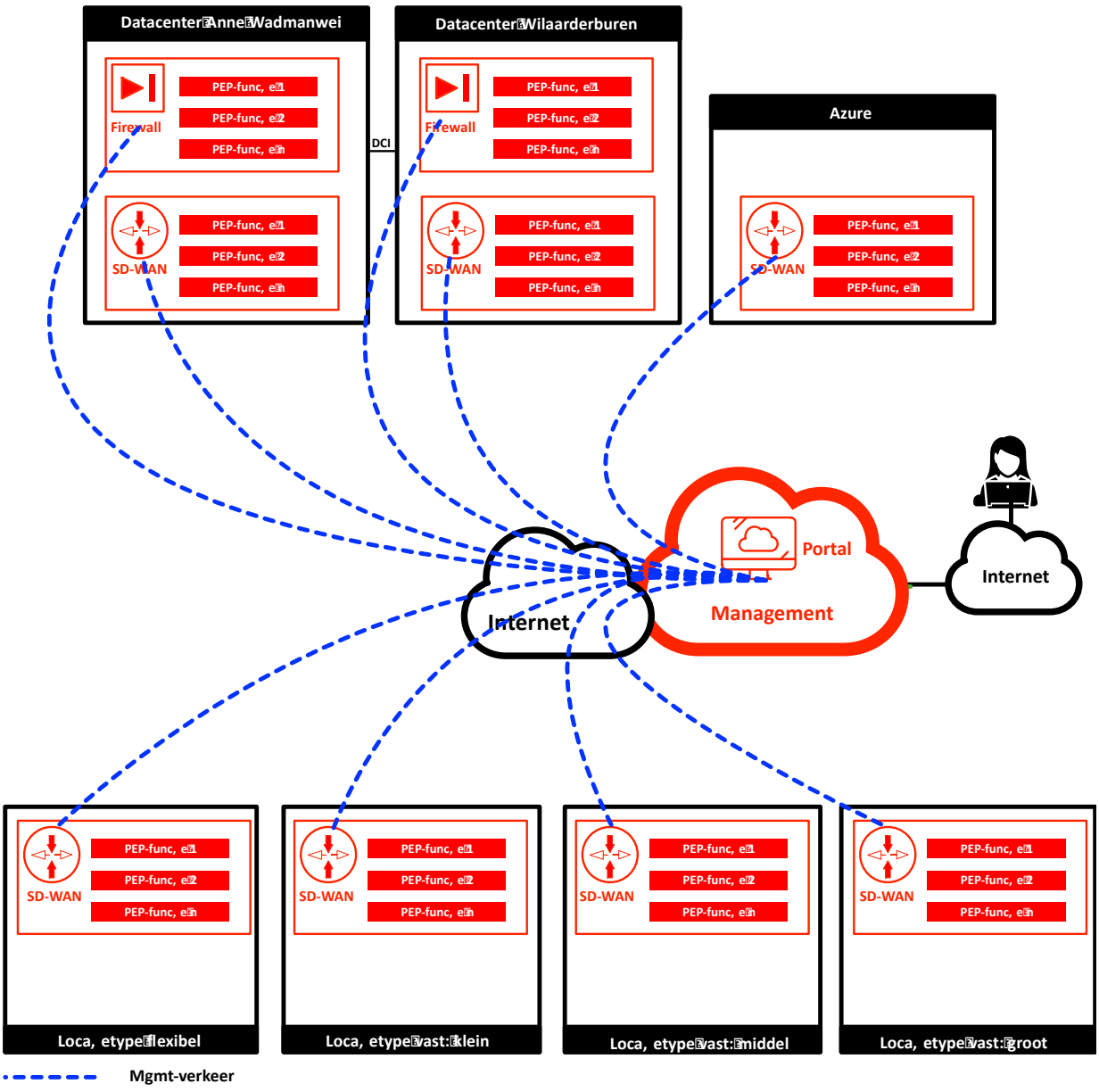
- Zonering/segmentatie,
- Encryptie WAN,
- Malware/virus defense,
- Web filtering,
- DNS filtering,
- Web Application Firewall,
- DDOS-protectie,
- Application Control,
- IPS/IDS.

Voor meer informatie over PEP-functies als 'bouwblokken' wordt verwezen naar paragaaf 4.3.

Let op: het is aan de winnaar van de aanbesteding het ROC te consulteren over aantallen/typen PEP-functies -> waar deze in te zetten o.b.v. vergelijkbare omgevingen.

3.2.10.3 Centraal management PEP-voorzieningen

Het is van belang om alle PEP-functies vanuit één platform te kunnen benaderen. Het voorkeursscenario hierbij is de inzet van een cloudplatform zoals afgebeeld in figuur 3-35. Mocht dit onverhoopt niet kunnen, is het mogelijk bepaalde managementtooling on-premises of in Azure onder te brengen. Integraliteit van de managementoplossing is echter van belang, zodat niet meerdere portals/ managementsystemen parallel moeten worden geraadpleegd voor een integraal overzicht en analyse van de PEP-voorzieningen en activiteiten/trends/issues in dit kader. Tevens is het van belang, dat centrale aanpassingen van rules simultaan worden gepushed naar alle firewall-nodes in het netwerk (i.e. centraal management van de oplossing en geen punt-oplossingen).



Figuur 3-35: *Centraal managementplatform voor PEP-functies*

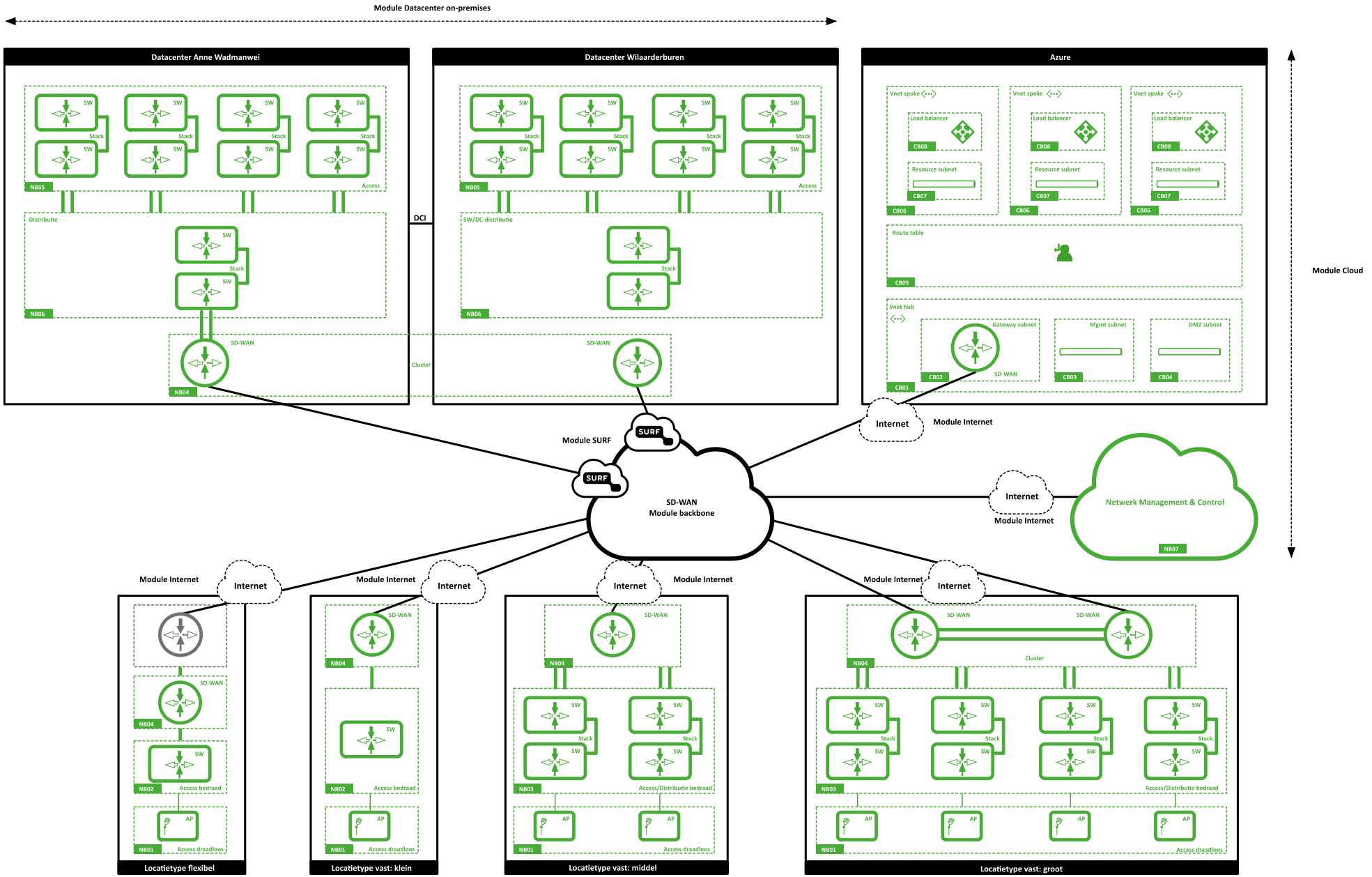
4 Logisch niveau (Hoe?)

Op logisch niveau wordt de ‘Hoe-vraag’ beantwoord (Hoe wordt de oplossing aangebracht? Uit welke bouwblokken bestaat de oplossing?). Uit het ontwerp in hoofdstuk 3 volgen de bouwblokken die nodig zijn om het einddoel te realiseren. In dit hoofdstuk wordt beschreven hoe deze bouwblokken worden toegepast. Er wordt hierbij een onderscheid gemaakt tussen:

- Non-cloudbouwblokken (on-premises bouwblokken),
- Cloudbouwblokken (Azure),
- Securitybouwblokken.

Elk bouwblok wordt beschreven in een aparte paragraaf. Het doel hiervan is dat in elke paragraaf een helder en overzichtelijke beschrijving staat voor een specifiek bouwblok.

Figuur 4-1 bevat de cloud- en non-cloudbouwblokken. Figuur 4-2 bevat de securitybouwblokken.



Figuur 4-1: *Overzicht non-cloud en cloudbouwblokken (netwerkperspectief)*

4.1 Non-cloudbouwblokken

De volgende Non-cloudbouwblokken worden onderkend:

Volgnr	Gerelateerde module	Naam Bouwblok in dit HLD
NB01	Locatie	Access draadloos
NB02	Locatie	Access bedraad (locatietypen vast: klein, flexibel)
NB03	Locatie	Access/distributie bedraad (locatietypen vast: middel, vast: groot)
NB04	Backbone/internet/SURF	SD-WAN
NB05	Datacenter on-premises	Access datacenter
NB06	Datacenter on-premises	Distributie datacenter
NB07	Cloud/internet	Netwerk Management en Control

4.1.1 NB01 Access draadloos

NB01 Access draadloos	
(Beknopte) Conceptuele beschrijving van het bouwblok	Het draadloze access-netwerk geeft draadloze clients toegang tot het ROC FP-netwerk en daarmee tot de services die het ROC FP biedt. Draadloze clients zijn onder meer CYOD-devices, BYOD-devices, IoT-devices e.d. Het bouwblok is verbonden aan het bedrade access-netwerk (NB02/NB03).
Kwaliteitskenmerken	• Het draadloze access-netwerk is schaalbaar, zodat het eenvoudig is access points toe te voegen of te verwijderen zonder dat dit (noemenswaardige) onderbrekingen oplevert voor de draadloze dienstverlening. • Het draadloze access-netwerk voorziet in Quality of Service-functies voor het kwalitatief kunnen onderscheiden van verschillende typen verkeersstromen die zich voordoen in het netwerk van ROC FP. QoS is een end-to-end paradigma waarbij QoS-functies (i.e. QoS-markeringen) naadloos aansluiten op het bedrade netwerk. • Het draadloze access netwerk voorziet in een naadloze roaming-functionaliteit die transparant is voor draadloze clients. • Het draadloze access-netwerk voorziet in voldoende dekking, zodat er geen blind spots c.q. verminderde performance bestaat. Dit aspect dient tijdens een site-survey te worden geanalyseerd (i.e. aantallen access points, inmetingen, dB-waarden e.d.). • Logging dient (ook) te kunnen worden verstuurd naar bijvoorbeeld een door het ROC beheerde centrale SIEM-omgeving of naar een door het ROC FP ingehuurde leverancier van een centrale SIEM-omgeving. Dit kan zowel een on-premises- als een Azure-dienst zijn.

	• De portalfunctie van het draadloze access-netwerk dient te kunnen integreren met de portal van de SD-LAN-omgeving en (bij voorkeur) met de portal van de SD-WAN-omgeving. Op deze manier ontstaat integraliteit van de oplossing in termen van single pane of glass. • Het beheer van het draadloze access-netwerk dient zoveel mogelijk geautomatiseerd/georchestreerd te zijn middels de controller-functie vanuit de cloud (i.e. middels een gebruiksvriendelijke portalfunctie). • Het draadloze access-netwerk is gebaseerd op 'zero-touch-provisioning'. • Vendor/product moet zich in de positie van 'leader' in de magic quadrants van Gartner bevinden.
Ontwerpkeuze **(OK01)**	(Maximum) aantal access points.
Toelichting	Zie het document 'ROC FP Poortbezettingen, dimensionering en SLA'.
Implicatie	In overleg met de markt moet worden vastgesteld: • Hoeveel draadloos verkeer zal worden afgehandeld (in de huidige setting, maar ook verdiscontering van trends als IoT, BYOD in vergelijkbare omgevingen als het ROC FP e.d.). • Welk type access point het beste past bij de use cases van het ROC FP (denk ook aan IoT). Het document 'ROC FP Poortbezettingen, dimensionering en SLA' vormt hiervoor de basis.
Ontwerpkeuze **(OK02)**	Koppeling aan het bedrade access netwerk geschiedt middels één fysieke interface
Toelichting	Access points zijn voorlopig middels één fysieke interface verbonden aan het bedrade access-netwerk. Om ervoor te zorgen dat de access points in de toekomst hoog beschikbaar zijn om de toenemende hoeveelheid aan verkeer te kunnen afhandelen (i.e. het gebruik van de WiFi-6-standaard, BYOD-gebruik, IoT-consumptie), dienen access points te beschikken over minimaal twee vaste interfaces die middels linkbundelingstechnologie simultaan netwerk-verkeer kunnen afhandelen.
Implicatie	Het aantal bedrade poorten/vaste poortbezetting neemt hierdoor toe.

4.1.2 NB02 Access bedraad (locatietypen vast: klein, flexibel)

NB02 Access bedraad (locatietypen vast: klein, flexibel)	
(Beknopte) Conceptuele beschrijving van het bouwblok	Het bedrade access-netwerk geeft bedrade clients, systemen en access points (NB01) toegang tot het ROC FP-netwerk en daarmee tot de services die het ROC FP biedt. Bedrade clients zijn onder meer printers, desktopsystemen, IoT-devices e.d. Het bouwblok is downstream verbonden aan het draadloze access-netwerk (NB01) en upstream aan de SD-WAN-oplossing (NB04).
Kwaliteitskenmerken	• Het bedrade access-netwerk is schaalbaar, zodat het eenvoudig is berade access nodes toe te voegen of te verwijderen zonder dat dit (noemenswaardige) onderbrekingen oplevert voor de bedrade dienstverlening. Dit betreft de horizontale schaalbaarheid. Verticale schaalbaarheid is hierbij ook een kwaliteitskenmerk. Uplinks/downlinks (i.e. bandbreedteverhoging/verlaging) dienen binnen de dienstverlening te vallen. Opwaardering vindt plaats op het niveau van het koppelvlak. Situationeel zal moeten worden vastgesteld of hierbij ook de gebouwbekabeling moet worden aangepast. • Het bedrade access-netwerk voorziet in Quality of Service-functies voor het kwalitatief kunnen onderscheiden van verschillende typen verkeersstromen die zich voordoen in het netwerk van ROC FP. QoS is een end-to-end paradigma waarbij QoS-functies (i.e. QoS-markeringen) naadloos aansluiten op de upstream netwerken en downstream netwerken. • Logging dient (ook) te kunnen worden verstuurd naar bijvoorbeeld een door het ROC beheerde centrale SIEM-omgeving of naar een door het ROC FP ingehuurde leverancier van een centrale SIEM-omgeving. Dit kan zowel een on-premises- als een Azure-dienst zijn. • De portalfunctie van het bedrade access-netwerk dient te kunnen integreren met de portal van de WiFi-omgeving en (bij voorkeur) met de portal van de SD-WAN-omgeving. Op deze manier ontstaat integraliteit van de oplossing in termen van single pane of glass. • Het beheer van het bedrade access-netwerk dient zoveel mogelijk geautomatiseerd/georchestreerd te zijn middels de controller-functie vanuit de cloud (i.e. middels een gebruiksvriendelijke portalfunctie). • Het bedrade access-netwerk is gebaseerd op ‘zero-touch-provisioning’. • Vendor/product moet zich in de positie van ‘leader’ in de magic quadrants van Gartner bevinden.

Ontwerpkeuze **(OK01)**	Multi-site-topologie (SDN)
Toelichting	Het SDN-model is gebaseerd op de principes van de 'multi-site', waarbij iedere locatie (SDN-fabric-site) is voorzien van een eigen set aan gelijkwaardige SDN-functionaliteiten (i.e. control plane en data plane functies). Dit in tegenstelling tot het SDN-model 'single site', waarbij in de regel op centrale sites (e.g. datacenters) de SDN-componenten zijn ondergebracht die control plane functies uitoefenen en op decentrale sites (e.g. de eindlocaties) de SDN-componenten die de data plane functies uitoefenen.
Implicatie	Middels het multi-site-model kunnen: • Alle locatietypen optimaal standalone functioneren. • De module backbone (i.e. SD-WAN) flexibel blijft indien deze wordt afgenomen als backbone as a service. De kans is immers aanwezig, dat leveranciers van SD-WAN-oplossingen de benodigde SD-LAN-communicatieprotocollen (dit kunnen proprietary protocollen zijn), niet ondersteunen indien de single site-topologie zou worden toegepast.

4.1.3 NB03 Access/distributie bedraad (locatietypen vast: middel, vast: groot)

NB03 Access/distributie bedraad (locatietpen vast: middel, vast: groot	
(Beknopte) Conceptuele beschrijving van het bouwblok	Het bedrade access-netwerk geeft bedrade clients, systemen en access points (NB01) toegang tot het ROC FP-netwerk en daarmee tot de services die het ROC FP biedt. Bedrade clients zijn onder meer printers, desktopsystemen, IoT-devices e.d.d. Het bouwblok is downstream verbonden aan het draadloze access-netwerk (NB01) en upstream aan het distributienetwerk. Het distributienetwerk is verbonden aan de SD-WAN-oplossing (NB04).
Kwaliteitskenmerken	• Het SD-LAN-netwerk (i.e. combinatie access en distributie) voorziet in Quality of Service. • Het SD-LAN-netwerk (i.e. combinatie access en distributie) is schaalbaar, zodat het eenvoudig is access nodes of distributienodes toe te voegen of te verwijderen zonder dat dit (noemenswaardige) onderbrekingen oplevert voor de bedrade dienstverlening. Dit betreft de horizontale schaalbaarheid. Verticale schaalbaarheid is hierbij ook een kwaliteitskenmerk. Uplinks/downlinks (i.e. bandbreedte-verhoging/verlaging) dienen binnen de dienstverlening te vallen. Opwaardering vindt plaats op het niveau van het koppelvlak. Situationeel zal moeten worden vastgesteld of hierbij ook de gebouwbekabeling moet worden aangepast.

	• Logging dient (ook) te kunnen worden verstuurd naar bijvoorbeeld een door het ROC beheerde centrale SIEM-omgeving of naar een door het ROC FP ingehuurde leverancier van een centrale SIEM-omgeving. Dit kan zowel een on-premises- als een Azure-dienst zijn. • De portalfunctie van het SD-LAN-netwerk (i.e. combinatie access en distributie) dient te kunnen integreren met de portal van de WiFi-omgeving en (bij voorkeur) met de portal van de SD-WAN-omgeving. Op deze manier ontstaat integraliteit van de oplossing in termen van single pane of glass. • Het beheer van het SD-LAN-netwerk (i.e. combinatie access en distributie) dient zoveel mogelijk geautomatiseerd/georchestreerd te zijn middels de controller-functie vanuit de cloud (i.e. middels een gebruiksvriendelijke portalfunctie). • Het SD-LAN-netwerk (i.e. combinatie access en distributie) is gebaseerd op 'zero-touch-privisioning'. • Vendor/product moet zich in de positie van 'leader' in de magic quadrants van Gartner bevinden.
Ontwerpkeuze **(OK01)**	Multi-site-topologie (SDN)
Toelichting	Zie NB02
Implicatie	Zie NB02
Ontwerpkeuze **(OK02)**	Ontsluiting naar de SD-WAN-oplossing is gebaseerd op linkbundelings-technologie.
Toelichting	Aangezien dit een middelgrote en grote locatie betreft is de hoeveelheid af te handelen verkeer groter dan op het locatietype vast: klein en flexibel. De ontsluiting van de distributielaag (of spine-laag) naar het SD-WAN is hierbij gebaseerd op link-bundelingstechnologie.
Implicatie	Er dient rekening te worden gehouden met meer patches (i.e. gebouwbeka-beling) tijdens de implementatiefase.
Ontwerpkeuze **(OK03)**	Stacking van nodes
Toelichting	Het SD-LAN-netwerk (i.e. combinatie access en distributie) dient te zijn gebaseerd op stack-mogelijkheden of op de leaf-spine-leaf-topologie die in de regel eigen is aan SD-LAN-topologieën.
Implicatie	Uitval van één van de nodes dient automatisch te worden opgevangen door verkeersafhandeling van de andere nodes (waar mogelijk).

4.1.4 NB04 SD-WAN

NB04 SD-WAN	
(Beknopte) Conceptuele beschrijving van het bouwblok	Het SD-WAN voorziet in connectiviteit tussen de locatietypen, het on-premises-datacenter en het cloud-datacenter. Het faciliteert in dezen alle communicatiestromen tussen voornoemde omgevingen. Tevens voorziet het SD-WAN in een decentrale internet breakout (DIA, Direct Internet Access) voor communicatiestromen die direct het internet dienen te gebruiken (e.g. regulier internet browsen, benaderen SaaS-diensten, benaderen remediation servers, update servers e.d.).
Kwaliteitskenmerken	• Het SD-WAN-netwerk is schaalbaar, zodat het eenvoudig is nieuwe nodes toe te voegen of te verwijderen zonder dat dit (noemenswaardige) onderbrekingen oplevert voor de dienstverlening. Dit betreft de horizontale schaalbaarheid (e.g. uitrol nieuwe locatie). Verticale schaalbaarheid is hierbij ook een kwaliteitskenmerk. Uplinks/downlinks (i.e. bandbreedteverhoging/ verlaging) dienen binnen de dienstverlening te vallen. Opwaardering vindt plaats op het niveau van het koppelvlak. Situationeel zal moeten worden vastgesteld of hierbij ook de gebouwbekabeling moet worden aangepast. • Het SD-WAN-netwerk voorziet in Quality of Service-functies voor het kwalitatief kunnen onderscheiden van verschillende typen verkeersstromen die zich voordoen in het netwerk van ROC FP. QoS is een end-to-end paradigma waarbij QoS-functies (i.e. QoS-markeringen) naadloos aansluiten op de upstream netwerken en downstream netwerken. • Logging dient (ook) te kunnen worden verstuurd naar bijvoorbeeld een door het ROC beheerde centrale SIEM-omgeving of naar een door het ROC FP ingehuurde leverancier van een centrale SIEM-omgeving. Dit kan zowel een on-premises- als een Azure-dienst zijn. • De portalfunctie van het SD-WAN-netwerk dient (bij voorkeur) te kunnen integreren met de portals van de WiFi-omgeving en SD-LAN-omgevingen. Op deze manier ontstaat integraliteit van de oplossing in termen van single pane of glass. • Het beheer van het SD-WAN-netwerk dient zoveel mogelijk geautomatiseerd/georchestreerd te zijn middels de controller-functie vanuit de cloud (i.e. middels een gebruiksvriendelijke portalfunctie). • Het underlay-netwerk dient te kunnen worden vormgegeven middels verschillende typen netwerktechnologieën, zijnde de dragers van het overlay netwerk (e.g. 4/5G, internet, MPLS et cetera).

	• Het SD-WAN-netwerk is gebaseerd op ‘zero-touch-privisioning’. • Vendor/product moet zich in de positie van ‘leader’ in de magic quadrants van Gartner bevinden.
Ontwerpkeuze **(OK01)**	Direct Internet Breakout (DIA)
Toelichting	Naarmate het ROC steeds meer gebruikmaakt van SaaS-toepassingen en door de toename van internet browsen in het algemeen, is het van belang de centrale internetopgang in het on-premises-datacenter en andere componenten aldaar (e.g. centrale firewallomgeving, maar ook het SD-WAN zelf) te ontlasten. Met ander woorden, hairpinning van verkeersstromen in het on-premises-datacenter wordt door de DIA voorkomen.
Implicatie	Door gebruik te maken van een DIA dienen security-functies ook decentraal te worden ingericht. Voor meer informatie wordt verwezen naar paragraaf. 4.3.
Ontwerpkeuze **(OK02)**	Clustering van nodes
Toelichting	Op het locatietype vast: groot zijn twee SD-WAN-nodes aangebracht. Deze nodes dienen simultaan verkeer te kunnen afhandelen in de hoedanigheid van een cluster. In ieder on-premises-datacenter wordt een SD-WAN-node aangebracht, waarbij clustering van de nodes ‘over de datacenters’ heen wordt aangebracht.
Implicatie	Hierbij moet gekozen kunnen worden om bepaalde verkeersstromen via het meest goedkope onderliggende fysieke medium (i.e. de fysieke drager) te kunnen afhandelen. Dit middels centraal aangebrachte policies in de controller.
Ontwerpkeuze **(OK03)**	Failback SD-WAN-netwerk on-premises-datacenter
Toelichting	Communicatie tussen applicaties/systemen tussen de twee on-premises-datacenters verloopt via de DCI (Datacenter Interconnect). Dit geldt ook voor communicatiestromen als heart beats tussen clusters van on-premises firewalls en de SD-WAN-nodes zelf. Indien het DCI-netwerk niet meer functioneert, dienen de SD-WAN-nodes de betreffende communicatie af te handelen.
Implicatie	Design topic, waarbij rekening moet worden gehouden met de routering van het netwerk.

4.1.5 NB05 Access datacenter

NB05 Access datacenter	
(Beknopte) Conceptuele beschrijving van het bouwblok	Het access-netwerk voorziet in toegang tot het netwerk voor serversystemen, backup & restore-systemen, storage-systemen.
Kwaliteitskenmerken	• Het access-netwerk is schaalbaar, zodat het eenvoudig is access nodes toe te voegen of te verwijderen zonder dat dit (noemenswaardige) onderbrekingen oplevert voor de dienst-verlening. Dit betreft de horizontale schaalbaarheid. Verticale schaalbaarheid is hierbij ook een kwaliteitskenmerk. Uplinks/downlinks (i.e. bandbreedteverhoging/verlaging) dienen binnen de dienstverlening te vallen. Opwaardering vindt plaats op het niveau van het koppelvlak. Situationeel zal moeten worden vastgesteld of hierbij ook de gebouwbekabeling moet worden aangepast. • Het access-netwerk voorziet in Quality of Service-functies voor het kwalitatief kunnen onderscheiden van verschillende typen verkeersstromen die zich voordoen in het netwerk van ROC FP. QoS is een end-to-end paradigma waarbij QoS-functies (i.e. QoS-markeringen) naadloos aansluiten op de upstream netwerken. • Logging dient (ook) te kunnen worden verstuurd naar bijvoorbeeld een door het ROC beheerde centrale SIEM-omgeving of naar een door het ROC FP ingehuurde leverancier van een centrale SIEM-omgeving. Dit kan zowel een on-premises- als een Azure-dienst zijn. • De portalfunctie van het access-netwerk dient te kunnen integreren met de portal van de WiFi-omgeving en (bij voorkeur) met de portal van de SD-WAN-omgeving. Op deze manier ontstaat integraliteit van de oplossing in termen van single pane of glass. • Het beheer van het access-netwerk dient zoveel mogelijk geautomatiseerd/georchestreerd te zijn middels de controller-functie vanuit de cloud (i.e. middels een gebruiksvriendelijke portalfunctie). • Het access-netwerk is gebaseerd op ‘zero-touch-privisioning’. • Vendor/product moet zich in de positie van ‘leader’ in de magic quadrants van Gartner bevinden.
Ontwerpkeuze **(OK01)**	Stacking van nodes

Toelichting	Het access-netwerk dient te zijn gebaseerd op stack-mogelijkheden of op de leaf-spine-leaf-topologie die in de regel eigen is aan SD-LAN-topologieën.
Implicatie	Uitval van één van de nodes dient automatisch te worden opgevangen middels verkeersafhandeling door de andere node. Systemen die worden ontsloten door het access netwerk zijn derhalve (bij voorkeur) verspreid over twee access nodes middels linkbundelingstechnologieën.

4.1.6 NB06 Distributie datacenter

NB06 Distributie datacenter	
(Beknopte) Conceptuele beschrijving van het bouwblok	Het distributie-netwerk accommodeert het access-netwerk, de centrale firewall-omgeving en de SD-WAN-nodes. Het distributienetwerk is derhalve een belangrijke spil in het web voor communicatiedoeleinden.
Kwaliteitskenmerken	• Het SD-LAN-netwerk (i.e. combinatie access en distributie) voorziet in Quality of Service. • Het SD-LAN-netwerk (i.e. combinatie access en distributie) is schaalbaar, zodat het eenvoudig is access nodes of distributienodes toe te voegen of te verwijderen zonder dat dit (noemenswaardige) onderbrekingen oplevert voor de dienstverlening. Dit betreft de horizontale schaalbaarheid. Verticale schaalbaarheid is hierbij ook een kwaliteitskenmerk. Uplinks/downlinks (i.e. bandbreedte-verhoging/verlaging) dienen binnen de dienstverlening te vallen. Opwaardering vindt plaats op het niveau van het koppelvlak. Situationeel zal moeten worden vastgesteld of hierbij ook de gebouwbekabeling moet worden aangepast. • Door verSaaSing van het applicatielandschap (i.e. cloud, tenzij strategie) neemt het aantal poorten in het on-premises-datacenter af. Op grond hiervan kan worden geconcludeerd dat er in principe geen separate core-omgeving noodzakelijk is maar gesproken kan worden van een ‘collapsed core’ model. • Logging dient (ook) te kunnen worden verstuurd naar bijvoorbeeld een door het ROC beheerde centrale SIEM-omgeving of naar een door het ROC FP ingehuurde leverancier van een centrale SIEM-omgeving. Dit kan zowel een on-premises- als een Azure-dienst zijn. • De portalfunctie van het SD-LAN-netwerk (i.e. combinatie access en distributie) dient (bij voorkeur) te kunnen integreren met de portal van de WiFi-omgeving en (bij voorkeur) met de portal van de SD-WAN-omgeving. Op deze manier ontstaat integraliteit van de oplossing in termen van single pane of glass.

	• Het beheer van het SD-LAN-netwerk (i.e. combinatie access en distributie) dient zoveel mogelijk geautomatiseerd/georchestreerd te zijn middels de controller-functie vanuit de cloud (i.e. middels een gebruiksvriendelijke portalfunctie). • Het SD-LAN-netwerk (i.e. combinatie access en distributie) is gebaseerd op 'zero-touch-privisioning'. • Vendor/product moet zich in de positie van 'leader' in de magic quadrants van Gartner bevinden.
Ontwerpkeuze **(OK01)**	Single site versus multi-site
Toelichting	De SDN-omgeving per datacenter site wordt beschouwd als een POD. Het ROC vraagt hierbij advies aan de markt of een single site of multi-site 'fabric' het beste past bij een scholengemeenschap. Hierbij moet ook rekening worden gehouden, dat het landschap van het ROC verSaaSt en dat het RCO een 'cloud-tenzij' strategie voert, waarbij IaaS-dienten op termijn in Azure worden ondergebracht.
Implicatie	N.v.t.
Ontwerpkeuze **(OK02)**	Stacking van nodes
Toelichting	Zie NB05
Implicatie	Zie NB05

4.1.7 NB07 Netwerk Management en Control

NB07 Netwerk Management en control	
(Beknopte) Conceptuele beschrijving van het bouwblok	Dit bouwblok voorziet in de aansturing van de WiFi-, SD-LAN en (bij voorkeur) SD-WAN-omgevingen. Met andere woorden: via één single-pane-of-glass wordt het gehele ROC-netwerk bestiert.
Kwaliteitskenmerken	• Gebruiksvriendelijke en intuïtieve interface, • Mogelijkheden om middels RBAC verschillende rollen toe te kennen met verschillende rechten (Het ROC krijgt een show-account voor inzage), • Single-pane-of-glass, • Automation & orchestration, • Self-healing-functies, • Application visibility & control, • Telemetrie, AI/ML (trendanalyse). • Vendor/product moet zich in de positie van 'leader' in de magic quadrants van Gartner bevinden.

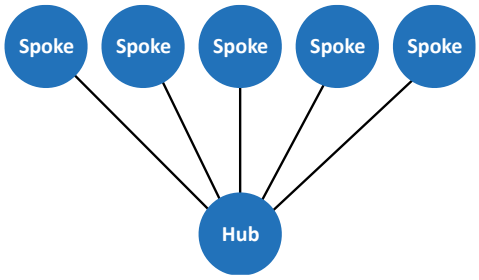
Ontwerpkeuze **(OK01)**	Cloudoplossing
Toelichting	Op grond van de ‘cloud, tenzij strategie’ die het ROC FP volgt wordt de management- en controle-oplossing voor het netwerk vanuit de cloud afgenomen.
Implicatie	Via het internet dient de portal van de cloudoplossing te kunnen worden benaderd. Dit maakt TPAW (Tijd-, Plaats-, Apparaatonafhankelijk werken) mogelijk c.q. eenvoudiger.
Ontwerpkeuze **(OK02)**	Keuze bestemming logging
Toelichting	Hoewel middels cloudtechnologie wordt gewerkt is het van belang, dat het ROC FP kan beschikken over alle logbestanden. Dit op grond van audit-verplichtingen.
Implicatie	Logging dient vanuit de beheerde netwerkcomponenten te kunnen worden verzonden naar een omgeving die het ROC opgeeft (e.g. SIEM-omgeving als on-premises-of Azure-dienst).

4.2 Cloudbouwblokken

De volgende Cloudbouwblokken worden onderkend:
[next release]

Volgnr	Naam Bouwblok in dit HLD
CB01	Vnet hub
CB02	SD-WAN
CB03	Mgmt. subnet
CB04	DMZ subnet
CB05	Route table
CB06	Vnet spoke
CB07	Resource subnet

4.2.1 CB01 Vnet hub

CB01 Vnet hub	
(Beknopte) Conceptuele beschrijving van het bouwblok	Net als een netwerk op een fysieke locatie, wordt een virtueel netwerk in Azure gebruikt als een middel om connectiviteit te bieden aan services die op het virtuele netwerk zijn aangesloten. Virtuele netwerken worden opgedeeld in een of meer virtuele subnetten waarmee de services daadwerkelijk zijn verbonden.
Kwaliteitskenmerken	Standaard Azure-dienstverlening.
Ontwerpkeuze **(OK01)**	Hub-and-spoke-topologie
Toelichting	De netwerktopologie binnen Azure is gebaseerd op de hub-and-spoke-topologie zoals afgebeeld in de onderstaande figuur.  Alle spoke-netwerken (spoke-Vnets) zijn verbonden aan het hub-netwerk (hub-Vnet).
Implicatie	Alle communicatie naar een spoke en tussen spokes verloopt via het hub-netwerk. Dit geldt ook voor verkeersstromen tussen systemen in verschillende spokes die tot dezelfde zone behoren en vallen in

	communicatiemodel 1. Dit vanuit het oogpunt van standaardisatie en het niet hoeven aan te leggen van spoke-spoke-relaties.
Ontwerpkeuze **(OK02)**	Shared resources
Toelichting	Gedeelde c.q. generieke resources als firewalling, DNS, domain controllers worden ondergebracht in het hub-netwerk.
Implicatie	Door het centraliseren van generieke resources worden kosten bespaard. Immers, er behoeven geen redundante resources te worden aangeschaft en ondergebracht in alle Vnets. Dit leidt ook tot een efficiënter management.

4.2.2 CB02 SD-WAN

Zie NB04 SD-WAN.

4.2.3 CB03 Mgmt. subnet

CB03 Mgmt. subnet	
(Beknopte) Conceptuele beschrijving van het bouwblok	Workloads zoals IaaS (VMs) in Azure moeten op een eenduidige en vellige manier worden beheerd. De meest eenvoudige oplossing is het gebruik van een jumpbox die wordt gehost in het Hub-vnet van de landingszone (i.e. subnet) voor gegevensbeheer (i.e. management). Een jumpbox is een Azure virtual machine (VM) waarop Linux of Windows draait en waarmee beheerders verbinding kunnen maken via het Remote Desktop Protocol (RDP) of Secure Shell (SSH) protocol.
Kwaliteitskenmerken	Standaard Azure-dienstverlening
Ontwerpkeuze **(OK01)**	Centraal management vanuit het hubVnet
Toelichting	Management van workloads wordt centraal belegd, hetzij via een jumphost in het managementsubnet hetzij via andere functies zoals Azure Bastion.
Implicatie	Het direct benaderen van worksloads wordt vermeden. Een centraal managementpunt wordt hierbij ingericht middels een separaat management-subnet.

4.2.4 CB04 DMZ-subnet

CB04 DMZ-subnet	
(Beknopte) Conceptuele beschrijving van het bouwblok	Specifieke workloads met een publieke zijde worden in een separaat DMZ-subnet aangebracht dat zich in het hubVnet bevindt.
Kwaliteitskenmerken	Standaard Azure-dienstverlening

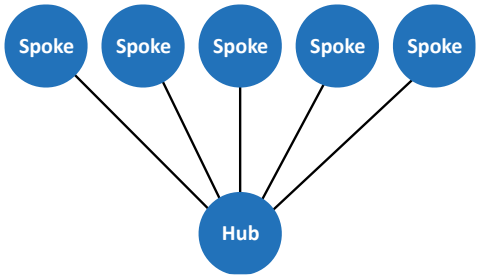
Ontwerpkeuze **(OK01)**	Benaderen DMZ-services via PEP-functies van de SD-WAN-node
Toelichting	Hoewel DMZ-services normaliter direct benaderbaar zijn vanaf het internet is het gebruikelijk om PEP-functies op communicatiestromen toe te passen.
Implicatie	De SD-WAN-node in het hubVnet dient de DMZ-verkeersstromen te controleren en waar nodig te blokkeren/filteren.

4.2.5 CB05 Route table

CB05 Route table	
(Beknopte) Conceptuele beschrijving van het bouwblok	Een routeringstabel is een set regels die wordt gebruikt om te bepalen welk pad IP-pakketten moeten volgen. Een dergelijke tabel bevat alle informatie die nodig is om het mogelijk te maken dat één of meerdere IP-pakketten over het netwerk worden getransporteerd via het beste netwerkpad. Aan een routetabel worden subnetten toegekend zie zijn aangemaakt in de vNets.
Kwaliteitskenmerken	Standaard Azuredienstverlening
Ontwerpkeuze **(OK01)**	UDR (User Defined Routes)
Toelichting	In Azure wordt gebruikgemaakt van handmatig aangepaste routes om: • de standaard systeemroutes van Azure te overschrijven, • extra routes toe te voegen aan de routetabel van een subnet.
Implicatie	Door het overschrijven van de standaard systeemroutes van Azure wordt ervoor gezorgd, dat verkeersstromen gedwongen worden te verlopen zoals het ROC FP deze voor ogen heeft. Dat wil bijvoorbeeld zeggen, dat de default route niet direct de Azure-internetopgang gebruikt maar wordt omgeleid naar de SD-WAN-node in het hubVnet. Op deze manier ontstaat maximale controle over verkeersstromen en kunnen de betreffende PEP-functies worden toegepast.

4.2.6 CB06 Vnet spoke

CB06 Vnet spoke	
(Beknopte) Conceptuele beschrijving van het bouwblok	Net als een netwerk op een fysieke locatie, wordt een virtueel netwerk in Azure gebruikt als een middel om connectiviteit te bieden aan services die op het virtuele netwerk zijn aangesloten. Virtuele netwerken worden opgedeeld in een of meer virtuele subnetten waarmee de services daadwerkelijk zijn verbonden.
Kwaliteitskenmerken	Standaard Azure-dienstverlening.

Ontwerpkeuze **(OK01)**	Hub-and-spoke-topologie
Toelichting	De netwerktopologie binnen Azure is gebaseerd op de hub-and-spoke-topologie zoals afgebeeld in de onderstaande figuur.  Alle spoke-netwerken (spoke-Vnets) zijn verbonden aan het hub-netwerk (hub-Vnet).
Implicatie	Alle communicatie naar een spoke en tussen spokes verloopt via het hub-netwerk. Dit geldt ook voor verkeersstromen tussen systemen in verschillende spokes die tot dezelfde zone behoren en vallen in communicatiemodel 1. Dit vanuit het oogpunt van standaardisatie en het niet hoeven aan te leggen van spoke-spoke-relaties.

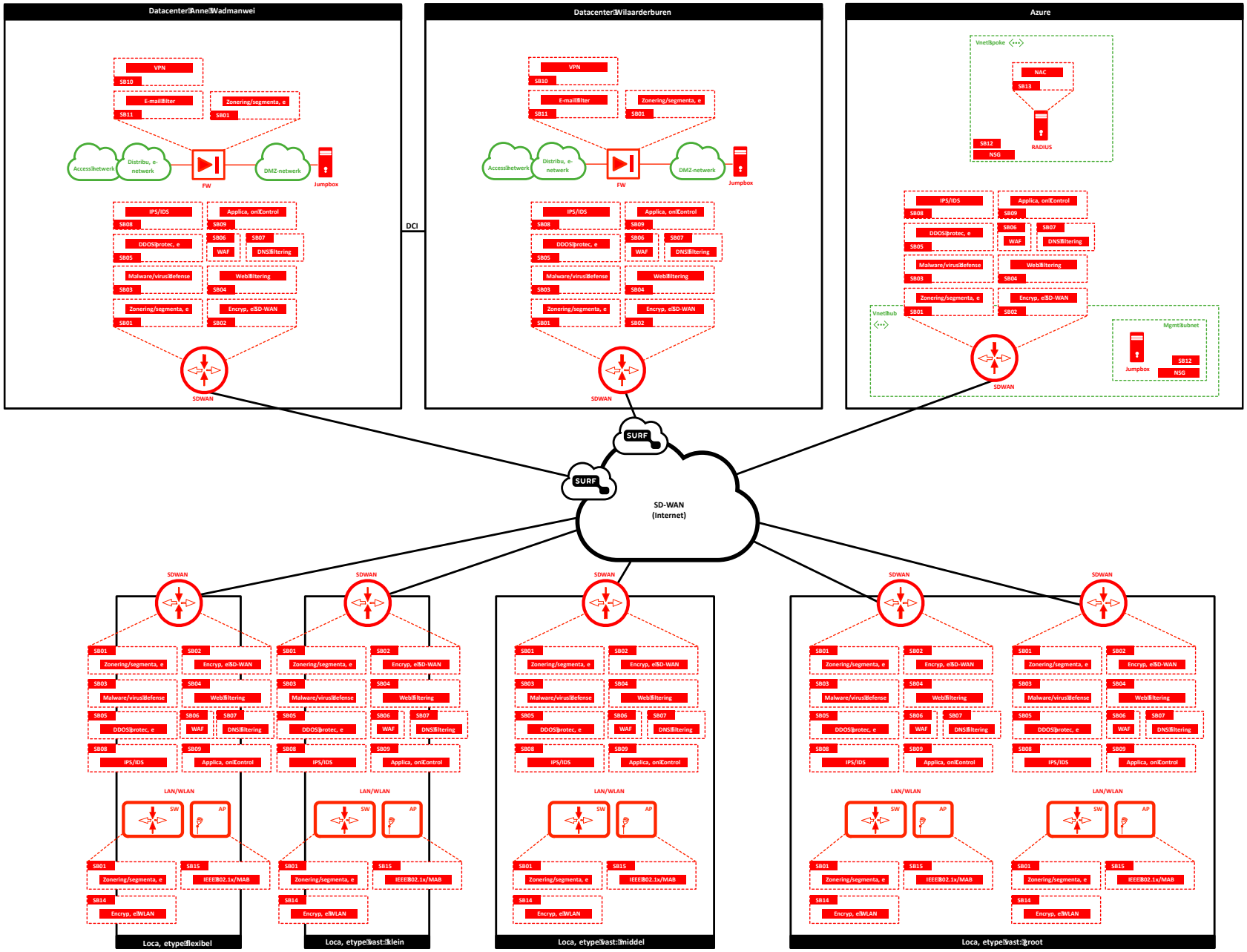
4.2.7 CB07 Resource subnet

CB07 Resource subnet	
(Beknopte) Conceptuele beschrijving van het bouwblok	Een resource subnet is een netwerkdeel waarbinnen Azure-resources als virtual machines (VM's) zijn opgenomen. Binnen een vNet kunnen (en zullen) meerdere subnetten aanwezig zijn.
Kwaliteitskenmerken	Standaard Azure-dienstverlening

4.2.8 CB08 Load balancer

CB08 Load balancer	
(Beknopte) Conceptuele beschrijving van het bouwblok	Azure Load Balancer werkt op laag 4 van het Open Systems Interconnection (OSI)-model. Een load balancer distribueert de inkomende verkeersstromen die aankomen bij de front-end-functie van de load balancer naar back-end pool-instanties (i.e. VMs).
Kwaliteitskenmerken	Standaard Azure-dienstverlening
Ontwerpkeuze **(OK01)**	Interne/private load balancer
Toelichting	Er wordt gebruikgemaakt van een private (en dus geen publieke) load balancer zodat de load balancer geen publieke IP-adressen hoeft te

	gebruiken. M.a.w.: interne/private load balancers worden gebruikt om verkeer binnen een een spoke-vnet te distribueren.
Implicatie	Vooralsnog gaat het ROC uit van het gebruik van één availability zone binnen de regio West-Europa, waardoor een publieke load balancer die verkeer distribueert tussen meerder availability zones niet noodzakelijk is. Zodra hier verandering in komt zal het HLD op dit punt worden aangepast.



Figuur 4-2: *Overzicht security-bouwblokken*

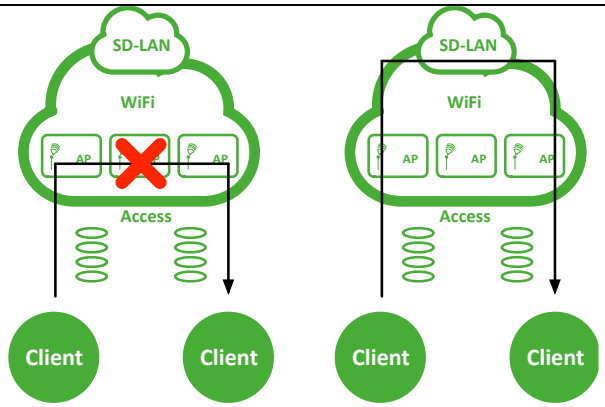
4.3 Security -bouwblokken

De volgende security-bouwblokken worden onderkend

Volgnr	Naam Bouwblok in dit HLD
SB01	Zonering/segmentatie
SB02	Encryptie SD-WAN
SB03	Malware / virus defense
SB04	Web filtering
SB05	DDOS protectie
SB06	Web Application Firewall
SB07	DNS filtering
SB08	IPS/IDS
SB09	Application Control
SB10	VPN
SB11	E-mail filtering
SB12	NSG
SB13	NAC
SB14	Encryptie WLAN
SB15	IEEE 802.1x/MAB

4.3.1 SB01 Zonering/segmentatie

SB01 Zonering/segmentatie	
(Beknopte) Conceptuele beschrijving van het bouwblok	Door het netwerk in te delen in zones is het mogelijk om gebruikers en systemen te classificeren op basis van vertrouwdheidniveaus. Door een zone verder op te delen in segmenten is het mogelijk risico's en kwetsbaarheden verder te isoleren. Directe communicatie tussen draadloze clients wordt geblokkeerd zoals in de onderstaande afbeelding is weergegeven. Communicatie tussen draadloze clients geschiedt via het SD-LAN-netwerk.

	
Kwaliteitskenmerken	• Het is mogelijk om een logische scheiding van verkeersstromen aan te brengen op grond van informatiebeveiligingsrichtlijnen van het ROC FP. • Het is mogelijk het zero-trust-model toe te passen op het netwerk middels host isolation/microsegmentatie. • Zonering/segmentatie is een end-to-end concept dat door het gehele netwerk van het ROC FP wordt toegepast. • P2P-blocking dient op SSID-niveau te kunnen worden toegepast.

Ontwerpkeuze **(OK01)**	Zero-trust-model
Toelichting	Het zero-trust-model zorgt voor de mogelijkheid om gebruikers en systemen van elkaar te isoleren. Dit middels microsegmentatie.
Implicatie	Het netwerk dient te voorzien in de mogelijkheid om microsegmentatie te kunnen toepassen. Dit dient derhalve op z'n minst tot de dienstverlening te behoren. Het is nog niet gezegd, dat het ROC FP dit op korte termijn doorvoert maar een voorbereiding hierop is wel van belang.

Ontwerpkeuze **(OK02)**	Segmentatie in relatie tot zonering
Toelichting	In theorie is het mogelijk om zonder PEP-functies communicatiestromen binnen dezelfde zone toe te staan. Het ROC FP kiest hier alleen per nader te definiëren gebruiksgevallen voor. Het ROC FP wil binnen een zone de controle houden over verkeersstromen door deze onder te brengen in één van de drie communicatiemodellen zoals beschreven in de paragraaf 3.2.8.2.
Implicatie	Zero-trust wordt toegepast (i.e. communicatiemodel 3 | secure private), zodat het netwerk dit dient te ondersteunen.

4.3.2 SB02 Encryptie SD-WAN

SB02 Encryptie SD-WAN	
(Beknopte) Conceptuele beschrijving van het bouwblok	SD-WAN-technologie maakt gebruik van IPsec. Aangezien de SD-WAN-oplossing gebruikmaakt van het publieke internet is een VPN- of IPsec-tunnel vereist om op z'n minst te voorkomen dat het verkeer tussen zender en ontvanger kan worden 'afgeluisterd' c.q. 'ontsleuteld'. De security-functie wordt gerealiseerd door: • Het authentiseren van de zender (i.e. zendende SD-WAN-node), de ontvanger (i.e. ontvangende SD-WAN-node) en de verkeersstroom (i.e. IP-pakketten) zelf die wordt 'verzonden', • Het delen van encryptiesleutels tussen de zender en de ontvanger, • Het gebruiken van het ESP-protocol (Encapsulating Security Payload) zodat verkeersstromen daadwerkelijk worden versleuteld, • Het gebruiken het AH-protocol (Authentication Header) waarmee de oorsprong van de verkeersstroom (i.e. IP-pakketten) wordt geverifieerd.
Kwaliteitskenmerken	Het toepassen van encryptie mag geen nadelige invloed hebben op de performance van het SD-WAN.
Ontwerpkeuze **(OK01)**	Gebruik van PKI-certificaten
Toelichting	Het SD-WAN kan worden beveiligd middels het gebruik van PKI-certificaten.
Implicatie	Indien gebruikgemaakt wordt van PKI-certificaten worden deze door de inschrijvende partij geleverd. Het ROC FP gaat uit van ontzorging.

4.3.3 SB03 Malware / virus defense (NGFW)

SB03 Malware / virus defense (NGFW)	
(Beknopte) Conceptuele beschrijving van het bouwblok	Een Next Generation Firewall maakt deel uit van de derde generatie firewalltechnologie en combineert een traditionele firewall (statefull firewalling, basis inspectie/filtering e.d) met andere geavanceerde technologieën. Geavanceerde technologiëen zijn bijvoorbeeld malware scanning, Advanced Persistent Threat Monitoring (ATM), virus defense e.d.
Kwaliteitskenmerken	• Functionaliteiten die deel uitmaken van de NG-suite moeten afzonderlijk c.q. *loosely coupled* zijn, zodat uitval van één NG-functie geen nadelige invloed heeft op andere NG-functies. • Uitval van een functie dient in de portal een alert te genereren. • Vendor/product moet zich in de positie van 'leader' in de magic quadrants van Gartner bevinden.

Ontwerpkeuze **(OK01)**	NGFW op SD-WAN-niveau
Toelichting	De SD-WAN-nodes voorzien in de functies die een NGFW biedt.
Implicatie	Doordat het SD-WAN de functie NGFW uitoefent, behoeven de centrale on-premises-firewalls niet over deze functie te beschikken. Alle verkeersstromen naar/vanaf het SD-WAN en internet verlopen immers via de SD-WAN-nodes.
Implicatie	Het is van belang geen overlap in PEP-functies te hebben tussen de SD-WAN-nodes en de centrale on-premises-firewall. Het ROC gaat hierbij uit van een advies van de markt over 'wat wijsheid in dezen is'. PEP-functies die het ROC voor ogen heeft zijn beschreven, maar in hoeverre een 'uitruil' van PEP-functies tussen de centrale on-premises firewalls en de SD-WAN-nodes noodzakelijk / verstandig is wordt aan de markt overgelaten.

4.3.4 SB04 Web filtering

SB04 Web filtering	
(Beknopte) Conceptuele beschrijving van het bouwblok	Client requests dienen rechtstreeks en automatisch te kunnen worden geblokkeerd op basis van: • Botnet-filter, • IPS/IDS, • Antivirus, • "Betrouwbare partij". Functies die concreet uitgevoerd moeten worden: • Blacklisting van client requests op grond van het beleid van het ROC FP, • Whitelisting van client requests op grond van het beleid van het ROC FP.

Kwaliteitskenmerken	• Client requests dienen alsnog te worden doorgelaten op grond van 'false positive' alerts.
	• Instelbaarheid van functies op grond van:
	  ○ Eén IP-adres,
	  ○ Subnet blocks,
	  ○ Land,
	  ○ Regio,
	  ○ Reputatie.
	• Uitval van de functie mag geen nadelige invloed hebben op de overige functies van de SD-WAN-nodes,
	• Uitval van een functie dient in de portal een alert te genereren.

	• Vendor/product moet zich in de positie van ‘leader’ in de magic quadrants van Gartner bevinden.
Ontwerpkeuze **(OK01)**	Web filtering op SD-WAN-niveau
Toelichting	De SD-WAN-nodes voorzien in de functie van web filtering
Implicatie	Doordat het SD-WAN de functie van Web filtering uitoefent, behoeven de centrale on-premises-firewalls niet over deze functie te beschikken. Alle verkeersstromen naar/vanaf het SD-WAN en internet verlopen immers via de SD-WAN-nodes. Het is van belang geen overlap in PEP-functies te hebben tussen de SD-WAN-nodes en de centrale on-premises-firewall. Het ROC gaat hierbij uit van een advies van de markt over ‘wat wijsheid in dezen is’. PEP-functies die het ROC voor ogen heeft zijn beschreven, maar in hoeverre een ‘uitruil’ van PEP-functies tussen de centrale on-premises firewalls en de SD-WAN-nodes noodzakelijk / verstandig is wordt aan de markt overgelaten.

4.3.5 SB05 DDOS protectie

SB05 DDOS protectie	
(Beknopte) Conceptuele beschrijving van het bouwblok	Een distributed-denial-of-service (DDoS)-aanval is een kwaadaardige poging om het reguliere verkeer vanaf/naar een server, service of netwerkonderdeel te verstoren door de target of de aanpalende infrastructuur te ‘overweldigen’ met een stortvloed aan internetverkeer. Functies van DDOS verhinderen of mitigeren in aanzienlijke mate dit type aanval.
Kwaliteitskenmerken	• Uitval van de functie mag geen nadelige invloed hebben op de overige functies van de SD-WAN-nodes, • Uitval van een functie dient in de portal een alert te genereren. • Vendor/product moet zich in de positie van ‘leader’ in de magic quadrants van Gartner bevinden.
Ontwerpkeuze **(OK01)**	DDOS-protectie op SD-WAN-niveau
Toelichting	De SD-WAN-nodes voorzien in de functie van DDOS-protectie
Implicatie	Doordat het SD-WAN de functie van DDOS-protectie uitoefent, behoeven de centrale on-premises-firewalls niet over deze functie te beschikken. Alle verkeersstromen naar/vanaf het SD-WAN en internet verlopen immers via de SD-WAN-nodes. Dit geldt dus ook voor de verschillende locatietypen waar gebruikgemaakt wordt van de decentrale internetuitbraak. Het is van belang geen overlap in PEP-functies te hebben tussen de SD-WAN-nodes en de centrale on-premises-firewall. Het ROC gaat hierbij uit van een

	advies van de markt over 'wat wijsheid in dezen is'. PEP-functies die het ROC voor ogen heeft zijn beschreven, maar in hoeverre een 'uitruil' van PEP-functies tussen de centrale on-premises firewalls en de SD-WAN-nodes noodzakelijk / verstandig is wordt aan de markt overgelaten.

4.3.6 SB06 WAF

SB06 WAF	
(Beknopte) Conceptuele beschrijving van het bouwblok	Een WAF beschermt web-apps door al het kwaadaardige HTTP/S-verkeer dat naar een webapplicatie verloopt te filteren, te bewaken en waar nodig te blokkeren en voorkomt hiermee, dat ongeautoriseerde gegevens de webapp verlaten. Een WAF beschermt de applicatielaag en is specifiek ontworpen om elk HTTP/S-verzoek op de applicatielaag te analyseren. Een WAF is in feite een intermediair tussen de gebruiker en de applicatie zelf, waarbij alle communicatie wordt geanalyseerd voordat deze de applicatie of de gebruiker bereikt. Instellingen worden doorgevoerd op grond van beleids-regels van het ROC FP.
Kwaliteitskenmerken	• Uitval van de functie mag geen nadelige invloed hebben op de overige functies van de SD-WAN-nodes, • Uitval van een functie dient in de portal een alert te genereren. • Vendor/product moet zich in de positie van 'leader' in de magic quadrants van Gartner bevinden.
Ontwerpkeuze **(OK01)**	WAF op SD-WAN-niveau
Toelichting	De SD-WAN-nodes voorzien in de functie van WAF
Implicatie	Doordat het SD-WAN de functie van WAF-protectie uitoefent, behoeven de centrale on-premises-firewalls niet over deze functie te beschikken. Alle verkeersstromen naar/vanaf het SD-WAN en internet verlopen immers via de SD-WAN-nodes. Dit geldt dus ook voor de verschillende locatietypen waar gebruikgemaakt wordt van de decentrale internetuitbraak. Het is van belang geen overlap in PEP-functies te hebben tussen de SD-WAN-nodes en de centrale on-premises-firewall. Het ROC gaat hierbij uit van een advies van de markt over 'wat wijsheid in dezen is'. PEP-functies die het ROC voor ogen heeft zijn beschreven, maar in hoeverre een 'uitruil' van PEP-functies tussen de centrale on-premises firewalls en de SD-WAN-nodes noodzakelijk / verstandig is wordt aan de markt overgelaten.

4.3.7 SB07 DNS filter

SB07 DNS filter	
(Beknopte) Conceptuele beschrijving van het bouwblok	Met DNS-filtering wordt de toegang tot bepaalde sites voor een specifiek doel c.q. specifieke categorie geblokkeerd. Doorgaans op basis van content filtering: e.g. o.b.v. een bepaalde site of categorie van sites die als bedreiging worden beschouwd. Middels het DNS-filter wordt het IP-adres van dergelijke sites geblokkeerd en de toegang ertoe verhinderd. Instellingen worden doorgevoerd op grond van beleidsregels van het ROC FP.
Kwaliteitskenmerken	• Uitval van de functie mag geen nadelige invloed hebben op de overige functies van de SD-WAN-nodes, • Uitval van een functie dient in de portal een alert te genereren. • Vendor/product moet zich in de positie van 'leader' in de magic quadrants van Gartner bevinden.
Ontwerpkeuze **(OK01)**	DNS-filter op SD-WAN-niveau
Toelichting	De SD-WAN-nodes voorzien in de functie van DNS filtering
Implicatie	Doordat het SD-WAN de functie van DNS filtering uitoefent, behoeven de centrale on-premises-firewalls niet over deze functie te beschikken. Alle verkeersstromen naar/vanaf het SD-WAN en internet verlopen immers via de SD-WAN-nodes. Dit geldt dus ook voor de verschillende locatietypen waar gebruikgemaakt wordt van de decentrale internetuitbraak. Het is van belang geen overlap in PEP-functies te hebben tussen de SD-WAN-nodes en de centrale on-premises-firewall. Het ROC gaat hierbij uit van een advies van de markt over 'wat wijsheid in dezen is'. PEP-functies die het ROC voor ogen heeft zijn beschreven, maar in hoeverre een 'uitruil' van PEP-functies tussen de centrale on-premises firewalls en de SD-WAN-nodes noodzakelijk / verstandig is wordt aan de markt overgelaten.

4.3.8 SB08 IPS/IDS

SB08 IPS/IDS	
(Beknopte) Conceptuele beschrijving van het bouwblok	De functie van Intrusion Prevention System (IPS) realiseert het op ongewenst gedrag kunnen monitoren van verkeersactiviteiten. De functie kan real-time reageren door het blokkeren (preventie) van dit ongewenste gedrag. De functie van Intrusion Detection System (IDS) realiseert de monitoring van gedrag (gewenst/ongewenst) zonder de functie van blokkeren (preventie) toe te passen. Met andere woorden: De functie heeft een signalerend karakter waarop een administrator wel/niet kan acteren.

	Met andere woorden: • Preventie van ongewenste verkeersactiviteiten (blokkades), • Detectie van gewenste/ongewenste verkeersactiviteiten (signalering).
Kwaliteitskenmerken	• De functie van IPS dient ongewenste verkeersactiviteiten te blokkeren, zonder daarbij het legitieme netwerkverkeer te blokkeren. • De functies van IPS en IDS dienen granulair te kunnen worden aangebracht, waarbij per applicatie, dienst, subnet kan worden aangegeven of IPS- en/of IDS-functies moeten worden toegepast. • Uitval van de functies van IPS/IDS mag geen nadelige invloed hebben op de overige functies van de SD-WAN-node. • Uitval van een functie dient in de portal een alert te genereren. • Vendor/product moet zich in de positie van 'leader' in de magic quadrants van Gartner bevinden.
Ontwerpkeuze **(OK01)**	IPS/IDS op SD-WAN-niveau
Toelichting	Aangezien wordt gekozen voor een DIA is het van belang, dat IPS/IDS-functies worden aangebracht.
Implicatie	Doordat het SD-WAN de functie van IPS/IDS uitoefent, behoeven de centrale on-premises-firewalls niet over deze functie te beschikken. Alle verkeers-stromen naar/vanaf het SD-WAN en internet verlopen immers via de SD-WAN-nodes. Het is van belang geen overlap in PEP-functies te hebben tussen de SD-WAN-nodes en de centrale on-premises-firewall. Het ROC gaat hierbij uit van een advies van de markt over 'wat wijsheid in dezen is'. PEP-functies die het ROC voor ogen heeft zijn beschreven, maar in hoeverre een 'uitruil' van PEP-functies tussen de centrale on-premises firewalls en de SD-WAN-nodes noodzakelijk / verstandig is wordt aan de markt overgelaten.

4.3.9 SB09 Application Control

SB09 Application Control	
(Beknopte) Conceptuele beschrijving van het bouwblok	Applicatie Control werkt door verschillende typen netwerkverkeer af te zetten c.q. te plotten op vooraf gedefinieerde modellen. Om systemen met elkaar te laten communiceren moet het netwerkverkeer aan bepaalde standaarden voldoen. Middels deze standaarden is de applicatiebeheerder in staat om verschillende typen verkeersstormen van elkaar te onderscheiden.

	Nadat een verkeersstroom is geïdentificeerd (i.e. behorende tot een bepaalde applicatie) kan deze worden geclassificeerd o.b.v.: Type: Applicaties kunnen worden geclassificeerd op basis van het doel. Dit kan helpen om de prioriteit van het verkeer te bepalen. Beveiligingsrisiconiveau: verschillende toepassingen brengen verschillende niveaus van cyberbeveiligingsrisico met zich mee. Protocollen die gegevens bevatten, zoals e-mail of FTP, kunnen bijvoorbeeld worden geclassificeerd als een hoog-risico vanwege de mogelijkheid van 'data exfiltration'. Het identificeren van deze risico's zorgt ervoor, dat veiligheidscontroles kunnen worden afgedwongen op basis van 'informed risk assessment'. Resourcegebruik: Sommige applicaties zijn veel meer 'resource-intensief' dan andere. Bijvoorbeeld: toepassingen voor videoconferenties, die zowel audio als video moeten 'live streamen', kunnen een grote hoeveelheid bandbreedte consumeren. Door dit type verkeer te identificeren kan ervoor worden gezorgd, dat het netwerk hierop wordt geoptimaliseerd. Implicaties voor productiviteit: sommige toepassingen, zoals applicaties voor sociale media, kunnen een positieve of negatieve invloed hebben op de productiviteit van medewerkers/studenten. Om deze reden kan op dit type verkeer worden gefilterd. Nadat een verkeersstroom is geïdentificeerd en gerelateerd aan een bepaalde applicatie kan het beleid van het ROC FP worden toegepast op de applicatie. Dit zorgt voor een hoog niveau van 'visibility & control' over t.a.v. de netwerkinfrastructuur.

Kwaliteitskenmerken	• Uitval van de functie mag geen nadelige invloed hebben op de overige functies van de SD-WAN-nodes,
	• Instelbaarheid t.a.v. het gedetecteerde netwerkverkeer:
	  ○ Verkeer moet kunnen worden geblokkeerd.
	  ○ Verkeer moet (alsnog) kunnen worden doorgelaten.
	• Uitval van een functie dient in de portal een alert te genereren.
	• Vendor/product moet zich in de positie van 'leader' in de magic quadrants van Gartner bevinden.

Ontwerpkeuze **(OK01)**	Application Control op SD-WAN-niveau
Toelichting	De SD-WAN-nodes voorzien in de functie van application control

Implicatie	Doordat het SD-WAN de functie van application control uitoefent, behoeven de centrale on-premises-firewalls niet over deze functie te beschikken. Alle verkeersstromen naar/vanaf het SD-WAN en internet verlopen immers via de SD-WAN-nodes. Het is van belang geen overlap in PEP-functies te hebben tussen de SD-WAN-nodes en de centrale on-premises-firewall. Het ROC gaat hierbij uit van een advies van de markt over 'wat wijsheid in dezen is'. PEP-functies die het ROC voor ogen heeft zijn beschreven, maar in hoeverre een 'uitruil' van PEP-functies tussen de centrale on-premises firewalls en de SD-WAN-nodes noodzakelijk / verstandig is wordt aan de markt overgelaten.

4.3.10 SB10 VPN

SB10 VPN	
(Beknopte) Conceptuele beschrijving van het bouwblok	De centrale on-premises-firewall voorziet in een VPN-module waarmee beheerders op afstand (e.g. thuis, mobility) en op een veilige manier de door hen beheerde IT-systemen kunnen benaderen.
Kwaliteitskenmerken	• Uitval van de functie mag geen nadelige invloed hebben op de overige functies van de on-premises firewall. • Uitval van een functie dient in de portal een alert te genereren. • Het VPN-gebruik mag geen nadelige impact hebben op de performance van de overige functies van de on-premises firewall. • Een VPN-sessie dient te zijn gelimiteerd in termen van bandbreedte-consumptie en levensduur.
Ontwerpkeuze **(OK01)**	PKI-certificaten
Toelichting	Voor authenticatiedoeleinden wordt gebruikgemaakt van publieke PKI-certificaten die zijn aangebracht op de centrale on-premises-firewall.
Implicatie	De inschrijver dient bij oplevering van het centrale on-premises firewall-cluster een publiek PKI-certificaat te leveren voor dit doeleinde.
Ontwerpkeuze **(OK02)**	SSL (TLS) en IPsec
Toelichting	Beide vormen van VPN-gebruik worden ondersteund: • Client VPN, • Site-2-site-VPN.
Implicatie	De firewall dient de meest veilige/recente versie van TLS te ondersteunen.

4.3.11 SB11 E-mail filter

SB11 E-mail filter	
(Beknopte) Conceptuele beschrijving van het bouwblok	Het filteren van e-mail zorgt ervoor, dat mailberichten worden 'gecontroleerd' die problematisch kunnen zijn als deze worden ontvangen en geopend door de ontvanger. Bijlagen worden hierbij gescanned en spam wordt hierbij teruggedrongen.
Kwaliteitskenmerken	• Uitval van de functie mag geen nadelige invloed hebben op de overige functies van de on-premises firewall. • Uitval van een functie dient in de portal een alert te genereren. • Het filter mag geen nadelige impact hebben op de performance van de overige functies van de on-premises firewall.
Ontwerpkeuze **(OK01)**	E-mail filter op on-premises-firewallniveau
Toelichting	De functie wordt in de centrale firewallomgeving aangebracht en niet op het SD-WAN. Echter, indien de markt aangeeft dat het 'beter' c.q. te adviseren is deze functie op het niveau van het SD-WAN (indien mogelijk) aan te brengen staat het ROC FP open voor dit advies.
Implicatie	N.v.t.

4.3.12 SB12 NSG

SB12 NSG	
(Beknopte) Conceptuele beschrijving van het bouwblok	Een Network Security Group (NSG) in Azure is de manier om een rule of accesslist (ACL) te activeren waarmee netwerkverkeer naar VMs (virtual machines) in een Vnet wordt toegestaan of geweigerd. NSGs kunnen ook worden gekoppeld aan subnetten of individuele VM's binnen het subnet. Rules/ACls worden beoordeeld op basis van prioriteit met behulp van de zogenaamde 5-tuple-informatie (bron, bronpoort, bestemming, bestemmingspoort en protocol) om het netwerkverkeer toe te staan of te weigeren.
Kwaliteitskenmerken	Standaard Azure-dienstverlening
Ontwerpkeuze **(OK01)**	Geen NSG in het gateway subnet (waar de SD-WAN-node is ondergebracht)
Toelichting	Dit is conform de best-practise van Azure.
Implicatie	Met referte aan: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings

4.3.13 SB13 NAC

SB13 NAC	
(Beknopte) Conceptuele beschrijving van het bouwblok	De centrale NAC (Network Access Control) oftewel RADIUS-server / Policy server is in de illlustratie aangebracht in de Azure-omgeving op grond van de 'cloud, tenzij strategie'. Aangezien Azure out-of-scope is voor de aanbesteding wordt de functionaliteit niet in Azure ondergebracht. Het is aan de markt vast te stellen of de functie als clouddienst kan worden afgenomen of in het on-premises-datacenter van het ROC FP moet worden ondergebracht. De RADIUS-server / Policy server ontvangt RADIUS-verzoeken van NAD (Network Access Devices als access switches, access points) waarbinnen IEEE 802.1x / MAB-verkeer wordt getunneld (i.e. het EAP-protocol). De RADIUS-server / Policy server zet het IEEE 802.1x / MAB-toegangsverleningsverzoek door naar de betreffende identity store van het ROC FP voor verificatie van de identiteit van de aanvrager.
Kwaliteitskenmerken	• Ondersteuning/integratie met Azure Active Directory, • Ondersteuning/integratie met Active Directory, • Ondersteuning/integratie met Intune, • Uitgebreide policyset / beleidsregels voor granulaire authenticatie- en autorisatiemogelijkheden, • Ondersteuning van BYOD-onboarding op een gebruiksvriendelijke wijze.
Ontwerpkeuze **(OK01)**	Redundante RADIUS-server/Policy server
Toelichting	Het is van belang, dat er geen SPOF ontstaat door slechts één RADIUS-server/Policy server in te zetten. Minimaal twee nodes dienen te zijn aangebracht.
Implicatie	Het exacte aantal nodes is afhankelijk van het aantal simultane RADIUS-sessies (i.e. het aantal te accommoderen NADs en bedrade/draadloze client) dat ondersteunt dient te worden. Het document 'ROC FP Poortbezettingen, dimensionering en SLA' levert hierbij input aan.
Ontwerpkeuze **(OK02)**	BYOD-portal
Toelichting	Het gebruik van BYOD neemt ook binnen het ROC FP toe. BYOD-devices die gebruik maken van services die het ROC FP biedt op de verschillende locatie-typen, de on-premises-datacenters en azure kunnen een verstoring/besmetting opleveren in het netwerk van het ROC FP. Immers, deze BYOD-devices zijn niet in beheer van het ROC FP.

Implicatie	BYOD onboarding moet mogelijk zijn in de NAC-omgeving middels portal-functies.

4.3.14 SB14 Encryptie WLAN

SB14 Encryptie WLAN	
(Beknopte) Conceptuele beschrijving van het bouwblok	Gegevensoverdracht tussen draadloze clients en access points dient te zijn versleuteld, zodat ongeautoriseerde partijen geen inzage hebben in onderhavige verkeersstromen.
Kwaliteitskenmerken	• Versleuteling/encryptie middels protocollen die in de draadloze netwerkbeveiligingspraktijk gangbaar zijn. • Versleuteling/encryptie dient voor gebruikers van het draadloze netwerk transparant te geschieden.

4.3.15 SB15 IEEE 802.1x / MAB

SB15 IEEE 802.1x / MAB	
(Beknopte) Conceptuele beschrijving van het bouwblok	In de bedrade en draadloze access-netwerken op de verschillende locatietypen is de PEP-functie IEEE 802.1x / MAB aangebracht. Dit houdt in, dat gebruikers van deze typen netwerken zich eerst dienen te authentiseren alvorens toegang wordt verkregen tot de netwerkomgeving van het ROC FP.
Kwaliteitskenmerken	• Ondersteuning van MAB voor devices die geen IEEE 802.1x ondersteunen. IEEE 802.1x is echter wel het voorkeursscenario. • MAB-toegang (waarbij het MAC-adres wordt gebruikt tijdens de authenticatie) dient te kunnen worden uitgebreid met device-specifieke kenmerken. Dit zodat de kans op het misbruik van alleen het MAC-adres (i.e. spoofing) wordt gemitigeerd. • De NAD dient RADIUS-sessies te kunnen opzetten naar verschillende RADIUS-servers/Policy servers, zodat het mogelijk is load balancing van toegangsverzoeken door te kunnen voeren.
Ontwerpkeuze **(OK01)**	PKI-certificaat/AuthC
Toelichting	In het kader van authenticatie van managed devices wordt bij voorkeur gebruikgemaakt van een PKI-certificaat.
Implicatie	Indien authenticatie middels een PKI-certificaat niet mogelijk is kan worden teruggevallen op MAB met device-specifieke karakteristieken die in combinatie in het authenticatieverzoek worden doorgegeven aan de RADIUS-/Policy server.

5 Appendix A: Gebruikte afkortingen

AAD:	Azure Active Directory
ACL:	Access list
AD:	Active Directory
AH:	Authentication Header
AI:	Artificial Intelligence
AP:	Access Point
ATM:	Advanced Persistent Threat Monitoring
AuthC:	Authentication
AuthZ:	Authorisation
BGP:	Border Gateway Protocol
BYOD:	Bring Your Own Device
CYOD:	Choose Your Own Device
Db:	Decibel
DCI:	Datacenter Interconnect
DCLAN:	Datacenter Local Area Network
DDOS:	distributed-denial-of-service
DIA:	Direct Internet Access
DMZ:	Demilitarized Zone
DNS:	Domain Name System
EAP:	Extensible Authentication Protocol
ESP:	Encapsulating Security Payload
FW:	Firewall
HLD:	High Level Design
IAAS:	Infrastructure As A Service
IAM:	Identity Access management
IDS:	Intrusion Detection System
IEEE:	Institute of Electrical and Electronics Engineers
IoT:	Internet of Things
IPS:	Intrusion Prevention System
IPsec:	Internet Security Protocol
ISE:	Identity Services Engine
LAN:	Local Area Network
MAB:	MAC Authentication Bypass
MAC:	Media Access Control
Mgmt:	Management
ML:	Machine Learning
NAAS:	Network As A Service
NAC:	Network Access Control
NAD:	Network Access Device

NAT:	Network Address Translation
NG:	Next Generation
NGFW:	Next Generation Firewall
NORA:	Nederlandse Overheids Referentie Architectuur
NSG:	Network Security Group (in Azure)
OSI:	Open Systems Interconnection
OTA:	Ontwikkel Test Acceptatie
P2P:	Point2Point
PAAS:	Platform As A Service
PDC:	Product Dienstencatalogus
PEP:	Policy Enforcement Point
PKI:	Public Key Infrastructure
PSK:	Preshared Key
QoS:	Quality of Service
RADIUS:	Remote Authentication Dial-In User Service
RDP:	Remote Desktop Protocol
ROC FP:	Regionaal Opleidingscentrum Friese Poort
SAAS:	Software As A Service
SD:	Software Defined
SD-LAN:	Software Defined Local Area Network
SD-WAN:	Software Defined Wide Area Network
SIEM:	Security Information Event Management
SSID:	Service Set Identifier
SLA:	Service Level Agreement
SPOF:	Single Point Of Failure
SSH:	Secure Shell
TPAW:	Tijd-, Plaats-, Apparaatonafhankelijk Werken
UDR:	User Defined Route
URL:	Uniform Resource Locater
VM:	Virtual Machine
Vnet:	Virtual network (in Azure)
VPN:	Virtual Private Network
WAF:	web Application Firewall
WAN:	Wide Area Network
WiFi:	Wireless Fidelity
WLAN:	Wireless Local Area Network

6 Appendix B: Uitwerking ontwerpregels architectuurblauwdruk architectuurgebied netwerk

[Zie document ‘Uitwerking ontwerpregels architectuurblauwdruk architectuurdomein netwerk]

7 Appendix B: Uitwerking ontwerpregels architectuurblauwdruk architectuurgebied security

[Zie document ‘Uitwerking ontwerpregels architectuurblauwdruk architectuurgebied security]